ACTA ARITHMETICA
XXIV (1973)

Some aspects of Gaussian composition

by

GORDON PALL* (Baton Rouge, La.)

Dedicated to Carl Ludwig Siegel on his seventy-fifth birthday

1. Introduction. At least two recent writers have described Gauss's theory of composition of binary quadratic forms as a tour de force, and not a few mathematicians have told me it was much too complicated to be of use. Although several writers (notably Smith, Arndt, and Pepin [2]) have published accounts of parts of the theory there has until recently been no persistent reconsideration of it. Apparently no one spent the time and effort needed fully to understand the Gaussian approach until my colleague, Hubert Butts, and I resolved to undertake this in 1968. Part of the reason for the lengthy delay was the circumstance that alternative simpler theories were available. The development of composition has tended to be dominated by the approaches of Dirichlet and Dedekind, both of whom were students of Gauss, and both of whom developed alternative methods which were simpler for the apparent objective than the Gaussian theory as it then was. It may now be said, without detracting in the least from the immense importance of the work of these men, that an early thoroughgoing reconsideration of Gauss's approach by means of suitably delimited bilinear substitutions might have led to a development of form theory in parallel with algebraic number theory which would have enriched mathematics. Further, Butts's researches into composition over various rings indicate that Gauss's approach generalizes better than the method of united forms. Furthermore, the bilinear substitutions have greater flexibility and versatility than the united forms, and have a wider range of applications.

2. Definition of Gaussian composition. Although Gauss dealt only with binary quadratic forms his definition has a natural extension to the norm forms of modules in algebraic fields. We will formulate the defi-

* This work was supported in part by N. S. F. grant GP 29105X.

nition for the more general case, but will confine ourselves after this section to the case $n = 2$.

We will call an n-ary n-ic form *primitive* if it has integer coefficients and represents integers prime to any desired nonzero integer. If $f = kg$ where g is primitive and k is a positive integer, we call k the *divisor of* f. We call an n-ary n-ic form f with rational coefficients *fully decomposable* (fd) if it is a product $L_1 L_2 \ldots L_n$ of linear forms $L_i = a_{i1}x_1 + \ldots + a_{in}x_n$ with coefficients a_{ij} in an algebraic extension F of the rationals. Permuting the L_i and multiplying them by factors in F with product 1 will permute the rows of the matrix

(1) $$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix},$$

and multiply them by the factors with product 1, but will not change the value of

(2) $$\partial(f) = |A|^2.$$

The quantity $\partial(f)$ can be shown to be rational, and to be integral if the coefficients of f are integers, and will be called the *discriminant of* f. If a linear transformation with the matrix T is applied to f, A is replaced by AT, hence $\partial(f)$ multiplied by $|T|^2$. Also, $\partial(cf) = c^2\partial(f)$ (c rational). A *class* is defined as consisting of all forms obtained from one by unimodular transformations (with integer coefficients and determinant 1).

Consider a bilinear substitution with integer coefficients p_i^{jk},

(3) $$x_i = \sum_{j,k=1}^{n} p_i^{jk} y_j z_k \qquad (i = 1, \ldots, n)$$

which sends an fd form f in the indeterminates x_i into a product of fd forms f' and f'' in the respective indeterminates y_j and z_k. One obtains a useful perspective by regarding the z_k (or y_j) as fixed, and so construing (3) as a linear transformation replacing f by kf' (or kf'') where k is the "constant" f'' (or f'). Since these transformations have the determinants

(4) $$\Delta_z = \Big|\sum_k p_i^{jk} z_k\Big|, \qquad \Delta_y = \Big|\sum_j p_i^{jk} y_j\Big|,$$

and the discriminants transform as above,

(5) $$\partial(f)(\Delta_z)^2 = f''^2\partial(f'), \qquad \partial(f)(\Delta_y)^2 = f'^2\partial(f'').$$

Equating the divisors of the forms on each side gives

(6) $$d'k''^2 = eh''^2, \qquad d''k'^2 = eh'^2,$$

where h', h'', k', k'' are the divisors of the respective forms $\Delta_y, \Delta_z, f', f''$, and e, d', d'' are the discriminants of f, f', f'' respectively.

Let f' and f'' be primitive, i.e., $k' = k'' = 1$. Then the y_j and z_k can be chosen to make f' and f'' prime to any desired nonzero integer, hence f is primitive. By (5) and (6),

(7) $$d' = eh''^2, \qquad d'' = eh'^2, \qquad \Delta_z = \pm h''f'', \qquad \Delta_y = \pm h'f'.$$

When $n = 2$, Gauss calls f a *compound* of the primitive forms f' and f'' if there exists a primitive bilinear substitution (3) making $f = f'f''$ and satisfying

(8) $$\Delta_z = h''f'', \qquad \Delta_y = h'f'.$$

(By so doing he obtained the class group familiar to all of us; with other sign choices in (8) one gets KL^{-1}, $K^{-1}L$, or $K^{-1}L^{-1}$, instead of KL.) Here "primitive" means that the six minor determinants of the matrix

(9) $$M = \begin{bmatrix} p_1^{11} & p_1^{12} & p_1^{21} & p_1^{22} \\ p_2^{11} & p_2^{12} & p_2^{21} & p_2^{22} \end{bmatrix}$$

of the bilinear substitution are coprime. Now the forms Δ_z and Δ_y are

(10) $$\Delta_z = [D_{13}, D_{14} + D_{23}, D_{24}], \qquad \Delta_y = [D_{12}, D_{14} - D_{23}, D_{34}],$$

where D_{ij} is the determinant with the i and j column of M. An odd prime p divides h' and h'' if and only if p divides every D_{ij}. This is true even if $p = 2$ since D_{14} and D_{23} cannot both be odd with the other D_{ij}'s even, because of the identity $D_{12}D_{34} - D_{13}D_{24} + D_{14}D_{23} = 0$. Hence if $n = 2$ the three properties

(11) $$M \text{ is primitive}, \qquad (h', h'') = 1, \qquad e = (d', d''),$$

are equivalent. When $n > 2$, the condition $(h', h'') = 1$ implies the primitivity of the bilinear substitution, and it seems better to define f to be a *Gaussian compound* of the primitive forms f' and f'' if $f = f'f''$ under a bilinear substitution (3) satisfying (8) and $(h', h'') = 1$. If $n > 2$ the existence of a Gaussian compound of f' and f'' requires that they have further properties in common.

In any case we can put $g' = h'f'$, $g'' = h''f''$, $g = h'h''f$, and can regard Gaussian composition as an operation on forms g', g'' of discriminant d ($= eh'^2h''^2$) with coprime divisors h', h'', yielding a product form of discriminant d and divisor $h'h''$.

3. We will show how to construct a Gaussian compound of the forms $[a, b, c]$, $[a', b', c']$ with the same discriminant d, coprime divisors, and $aa' \neq 0$. Anyone familiar with united forms might guess our construction from the following heuristic considerations. If $a = qm$ and $a' = qm'$ and

$b' \equiv -b \pmod{2q}$, then $[qm, b, c]$ and $[qm', b', c']$ seem to factor as $[q, b, cm][m, b, cq]$ and $[q, b', c'm'][m', b', c'q]$; and since $b' \equiv -b \pmod{2q}$, $[q, b, cm]$ and $[q, b', c'm']$ ought to cancel.

This suggests putting $q = (a, a', \frac{1}{2}(b+b'))$, $a = qm$, $a' = qm'$, and trying as a possible product $[mm', b'', \cdot]$. Now $a(ax^2+bxy+cy^2)$ factors as the product of $ax+\frac{1}{2}(b+\sqrt{d})y$ and its conjugate. Hence we are led to try

$$(12)\quad \big(ax+\tfrac{1}{2}(b+\sqrt{d})y\big)\big(a'x'+\tfrac{1}{2}(b'+\sqrt{d})y'\big) = q\big(mm'x''+\tfrac{1}{2}(b''+\sqrt{d})y''\big).$$

Multiplying this by its conjugate we get, if $d = b''^2-4mm'c''$,

$$(13)\qquad (ax^2+bxy+cy^2)(a'x'^2+b'x'y'+c'y'^2) = mm'x''^2+b''x''y''+c''y''^2.$$

Equating rational and irrational parts in (12) gives

$$(14)\qquad \begin{aligned} x'' &= qxx'+\frac{b'-b''}{2m'}xy'+\frac{b-b''}{2m}x'y+\frac{bb'+d-b''(b+b')}{4qmm'}yy',\\ y'' &= mxy'+m'x'y+\frac{b+b'}{2q}yy', \end{aligned}$$

where the coefficients will be integers if and only if

$$(15)\qquad \begin{gathered} b'' \equiv b' \pmod{2m'},\qquad b'' \equiv b \pmod{2m},\\ (b+b')b'' \equiv bb'+d \pmod{4qmm'}. \end{gathered}$$

By (15), c'' is an integer since $d-b''^2 \equiv (b-b'')(b''-b') \equiv 0 \pmod{4mm'}$. Also, (15) is equivalent to

$$(16)\quad mb'' \equiv mb',\qquad m'b'' \equiv m'b,\qquad \frac{b+b'}{2q} \equiv \frac{bb'+d}{2q} \pmod{2mm'},$$

where $bb'+d = b(b'+b)-4ac \equiv 0 \pmod{2q}$. It can be verified that (15) has a unique solution b'' mod $2mm'$ by use of the following lemma (given in [3], p. 134).

Lemma 1. *Let $(s, t_1, \ldots, t_n) = 1$. If s divides every $t_iq_j-t_jq_i$ $(i, j = 1, \ldots, n)$, there is one and only one solution b'' mod s of*

$$t_1b'' \equiv q_1,\quad \ldots,\quad t_nb'' \equiv q_n \pmod{s}.$$

Forming Δ_y and Δ_z we find that (14) is Gaussian.

It is well-known that every unimodular automorph of a primitive form $[a, b, c]$ of nonsquare discriminant d is expressed by

$$ax+\tfrac{1}{2}(b+\sqrt{d})y = \big(ax'+\tfrac{1}{2}(b+\sqrt{d})y'\big)\cdot\tfrac{1}{2}(t+u\sqrt{d}),$$

where t, u are any integer solutions of $t^2-du^2 = 4$. From this and from Theorem 3 which we are about to prove will follow at once that

Theorem 1. *Every Gaussian substitution under which (12) holds is given by*

$$\big(ax+\tfrac{1}{2}(b+\sqrt{d})y\big)\big(a'x'+\tfrac{1}{2}(b'+\sqrt{d})y'\big) = q\big(mm'x''+\tfrac{1}{2}(b''+\sqrt{d})y''\big)\cdot\tfrac{1}{2}(t+u\sqrt{d_0}),$$

where d_0 is the discriminant of the primitive part of $[mm', b'', c'']$, and t, u are any integral solutions of $t^2-d_0u^2 = 4$.

In August 1968, I raised and partially answered the question of how unique the Gaussian bilinear substitution is when the three forms f, f', f'' are fixed. I then searched the literature on this matter. The only thing I was able to find was a conjecture by Arndt something like Theorem 1; this conjecture was omitted by Mathews [5] in his account of Arndt's work, but it is given in Dickson's History.

We will now prove simultaneously two theorems:

Theorem 2. *The Gaussian compounds of forms in a class K by forms in a class L, where K and L have discriminant d and coprime divisors h' and h'' form a unique class KL, of discriminant d and divisor $h'h''$.*

Theorem 3. *Choose f' in K, f'' in L, f in KL, where K and L have discriminant d and coprime divisors. If M is the matrix of a Gaussian substitution under which $f = f'f''$, then every such matrix is given by WM, where W is an arbitrary unimodular automorph of f.*

Lemma 2. *If (3) holds, and $(y_1, y_2) = (z_1, z_2) = \big(f'(y_1, y_2), f''(z_1, z_2)\big) = 1$, then $(x_1, x_2) = 1$.*

Proof. The values of f' and f'' are now the determinants Δ_y and Δ_z. If p divides x_1, x_2 but not Δ_y or Δ_z, then p divides (y_1, y_2) or (z_1, z_2).

Lemma 3. *As is well-known we can choose in K and L united forms $[a_1, b, a_2c]$, $[a_2, b, a_1c]$ with $(a_1, a_2) = 1$. For forms f', f'' so chosen, if f is a Gaussian compound of f' and f'', f is in the class of $[a_1a_2, b, c]$.*

Proof. Take $y_1, y_2, z_1, z_2 = 1, 0, 1, 0$ in (3). Then $(x_1, x_2) = 1$ and $f(x_1, x_2) = a_1a_2$. Let T be a unimodular matrix with x_1, x_2 as first column. The representation x_1, x_2 by f *corresponds* to the representation $(x_1\ x_2)T'^{-1} = 1, 0$ by $f^T = [a_1a_2, \ldots, \ldots]$. Thus now $p_1^{11} = 1$, $p_2^{11} = 0$. The conditions $\Delta_y = f'$, $\Delta_z = f''$ now give

$$(17)\qquad \begin{aligned} &p_2^{12} = a_1, && p_2^{22}+p_1^{21}a_1-p_1^{12}a_2 = b, && p_1^{21}p_2^{22}-p_1^{22}p_2^{21} = a_2c,\\ &p_2^{21} = a_2, && p_2^{22}+p_1^{12}a_2-p_1^{21}a_1 = b, && p_1^{12}p_2^{22}-p_1^{22}p_2^{12} = a_1c. \end{aligned}$$

Thus $p_1^{21}a_1-p_1^{12}a_2 = 0$, and since $(a_1, a_2) = 1$, $p_1^{12} = ha_1$ and $p_1^{21} = ha_2$ where h is an integer. Thus $b = p_2^{22}$, $c = hb-p_1^{22}$, and

$$M = \begin{bmatrix} 1 & ha_1 & ha_2 & hb-c\\ 0 & a_1 & a_2 & b \end{bmatrix}.$$

Replacing x_1 by x_1+hx_2 replaces M by

$$\begin{bmatrix} 1 & 0 & 0 & -c \\ 0 & a_1 & a_2 & b \end{bmatrix}, \tag{18}$$

which makes $f=[a_1a_2, b, c]$. Theorem 2 follows. Notice that we can absorb this last translation into T at the beginning of this proof, and say there that a matrix T with x_1, x_2 as first column can be chosen so that $f^T=[a_1a_2, b, c]$.

Consider now any other Gaussian substitution under which $f=f'f''$, where $f=[a_1a_2, b, c]$, $f'=[a_1, b, a_2c]$, $f''=[a_2, b, a_1c]$. Then the same procedure yields a matrix W^{-1} which transforms f into f, whence M in (18) is replaced by WM.

To extend this to equivalent forms consider first two matrices M and M^* for $f=f'^U\cdot f''$, U unimodular. Let T denote U^{-1}. Applying T performs certain operations on M and M^*. Specifically for (3) it multiplies

$$\begin{bmatrix} p_1^{11} & p_1^{21} \\ p_2^{11} & p_2^{21} \end{bmatrix} \text{ and } \begin{bmatrix} p_1^{11} & p_1^{22} \\ p_2^{11} & p_2^{22} \end{bmatrix} \quad \text{on the } \textit{right} \text{ by } T.$$

By what we proved above, the new M^* can be formed by multiplying the new M on the *left* by a unimodular automorph of f. Since the right and left operations commute, we can apply U to f' again and have Theorem 3 for f, f'^U, f''. Similarly we can replace f'' by f''^U. Finally, replacing f by f^U, we first apply U^{-1} to f^U thus multiplying M on the left by U, then by a unimodular automorph W of f, then by U^{-1}; in all we have thus multiplied M on the left by $U^{-1}WU$, which is *any* unimodular automorph of f^U.

COROLLARY. *The change in M due to applying a unimodular automorph to f' or f'' can be obtained instead by multiplying on the left by some unimodular automorph of f.*

To prove that composition is associative choose in classes C_1, C_2, C_3 with discriminant d and divisors coprime in pairs, forms $[a_1, b, a_2a_3c]$, $[a_2, b, a_1a_3c]$, $[a_3, b, a_1a_2c]$. Clearly, both $(C_1C_2)C_3$ and $C_1(C_2C_3)$ contain $[a_1a_2a_3, b, c]$. One sees easily that the primitive classes of discriminant d form a group, and those of all the discriminants d_0s^2 (d_0 fundamental, s ranging over the positive integers) a semigroup.

4. Multiplication or factorization of representations. In (3) we can regard y_1, y_2 as a representation of some number n' by f', z_1, z_2 as a representation of some number n'' by f'', and x_1, x_2 as a *product representation* of $n'n''$ by f. By an *autoset* (automorphic set) of n by f we mean the set of representations obtained by applying to one the unimodular automorphs of f. Corresponding automorphic sets (by f and f^U), the *divisor* of a autoset (g.c.d. of x_1, x_2), *primitive* — have obvious meanings. The first thing Gauss did on binary quadratic forms (Sec. V of the D. A.) was to give an algorithm which associates with corresponding primitive autosets of n by the forms of a class a solution u modulo $2n$ of $u^2\equiv d \pmod{4n}$; or with the corresponding autoset containing 1, 0, by $[n, u, \ldots]$.

We may designate the autoset by f containing x_1, x_2 by the symbol $S(x_1, x_2; f)$, and may replace it by $S(t_1, t_2; g)$ if f and g are in the same class and the representations correspond. We may write

$$S(x_1, x_2; f)=S(y_1, y_2; f')\cdot S(z_1, z_2; f'') \tag{19}$$

to indicate that f is a Gaussian compound of f' and f'', and that under any Gaussian substitution which makes $f=f'f''$, the autoset on the left is the product of the representations on the right.

We assume hereafter that all forms are primitive and of discriminant d.

THEOREM 4. *Let the primitive representation y_1, y_2 of n' by f' belong (under Gauss's algorithm) to u'* $\pmod{2n'}$, *and let the primitive representation z_1, z_2 of n'' by f'' belong to u''* $\pmod{2n''}$. *Then the product representation has the* g.c.d. $q=\left(n', n'', \tfrac{1}{2}(u'+u'')\right)$.

Proof. If we use (14) to find the Gaussian compound of $[n', u', \cdot]$ and $[n'', u'', \cdot]$, and put $x, y, x', y' = 1, 0, 1, 0$, we get $x''=q$, $y''=0$. (The notations need adjusting.)

We may refer to the number represented as the *norm of the representation*. Consider a primitive representation of norm n belonging to u, and the corresponding $S(1, 0; [n, u, k])$. If $n=n_1n_2$, the two forms $[n_1, u, kn_2]$ and $[n_2, u, kn_1]$ will be primitive if and only if (n_1, n_2) has no bad prime factor p, i.e., such that d/p^2 is a discriminant. Assuming that they have no bad prime factor,

$$S(1, 0; [n_1n_2, u, k])=S(1, 0; [n_1, u, n_2k])\cdot S(1, 0; [n_2, u, n_1k]). \tag{20}$$

THEOREM 5. *The divisor of norm n_1 of a primitive representation of norm n_1n_2 is uniquely determined up to equivalence if (n_1, n_2) has no bad prime factor.*

Proof. We need only show that we cannot have

$$S(1, 0; [n_1n_2, u, k])=S(1, 0; [n_1, u_1, c_1])\cdot S(1, 0; [n_2, u_2, c_2]), \tag{21}$$

except when $u_1\equiv u \pmod{2n_1}$ and $u_2\equiv u \pmod{2n_2}$. Since by (21) the g.c.d. of the product representation is $1, \left(n_1, n_2, \tfrac{1}{2}(u_1+u_2)\right)=1$. Hence $q=1$ in (14), $n_1=m$, $n_2=m'$, and (15) gives $u\equiv u_1 \pmod{2n_1}$, $u\equiv u_2 \pmod{2n_2}$.

Repeated application of this shows that *a primitive representation can be expressed uniquely as a product of representations of prime norm, except that powers of bad primes must be left unbroken.*

One can proceed at this point to define prime representations by the primitive forms of discriminant d, and obtain a theory of unique factorization into primes, very much like theory of ideals in quadratic orders. I will not go into this here, but will merely remark that this could have been done on the basis of Gaussian composition long before ideals were actually discovered.

5. Application of Gaussian composition to writing formulas giving all solutions of certain diophantine equations, often with no solution occurring more than once. Our principal tool for this purpose is Theorem 5. First, let us consider Mordell's equation $x^2+e=z^3$. A first step in solving this equation is to write the solutions of $x^2+ey^2=z^3$ with $(x,y)=1$. There are methods in the literature which have been used for this purpose, but none (the author believes) are as good as what should have been the original method: Gaussian composition.

Let us consider rather the equation

$$(22)\qquad av_1^2+bv_1v_2+cv_2^2=n^k,\quad (v_1,v_2)=1,\quad (a,b,c)=1,\ k>1,$$

where the variables are v_1, v_2, and n. The case where n has bad prime factors can be reduced to cases where it does not, and we will here assume it does not. Notice that (22) asserts that the primitive autoset $S(v_1,v_2;f)$ (where $f=[a,b,c]$) has norm n^k, and by Theorem 5 the divisors of norm n can all be taken equal. Find first the primitive classes L of discriminant d such that $L^k=F$ (the class of f). In each such class L choose a form $[r,\cdot,\cdot]$ with r prime to d, and then by a translation obtain a form $[r,s,r^{k-1}t]$. For each i $(=1,\ldots,k-1)$,

$$(23)\qquad \big(r^iy_1+\tfrac{1}{2}(s+\sqrt{d})y_2\big)\big(rz_1+\tfrac{1}{2}(s+\sqrt{d})z_2\big)=r^{i+1}u_1+\tfrac{1}{2}(s+\sqrt{d})u_2$$

is easily seen to be a Gaussian product. Hence we can solve

$$(24)\qquad r^ku_1+\tfrac{1}{2}(s+\sqrt{d})u_2=\big(rx_1+\tfrac{1}{2}(s+\sqrt{d})x_2\big)^k$$

for u_1 and u_2 to obtain a family of solutions of

$$(25)\qquad r^ku_1^2+su_1u_2+cu_2^2=n^k,\quad \text{with}\quad n=rx_1^2+sx_1x_2+r^{k-1}tx_2^2.$$

At this point we should apply to u_1 and u_2 the unimodular automorphs of the form $[r^k,s,t]$. If d is a positive nonsquare integer the number of these is infinite, but we need only use the powers up to the $(k-1)$th power of the fundamental automorph, and their negatives. We can find a unimodular transformation carrying $[r^k,s,t]$ into $[a,b,c]$, and thus obtain corresponding formulas for v_1, v_2 in terms of x_1, x_2. To obtain coprime v_1, v_2, we need only restrict x_1, x_2 to be coprime and to be such that n in (25) is prime to d. (If $p\,|\,d$, powers of a representation with norm divisible by p are imprimitive (Theorem 4).)

References

[1] Hubert S. Butts and Bill J. Dulin, *Composition of binary quadratic forms over integral domains*, Acta Arith. 20 (1972), pp. 223–251.

[2] L. E. Dickson, *History of the Theory of Numbers*, vol. 3, pp. 60–79. References to F. Arndt, Dedekind, Dirichlet, T. Pepin, and H. J. S. Smith may be found here. Also, of course, Carl Friedrich Gauss.

[3] — *Introduction to the Theory of Numbers*, Chicago 1929; reprinted by Dover, 1957.

[4] I. Kaplansky, *Composition of binary quadratic forms*, Studia Math. 31 (1968), pp. 523–530.

[5] G. B. Mathews, *Theory of Numbers* (reprint), New York 1927.

Received on 8. 12. 1972 (359)