ON THE ARITHMETIC OF QUATERNIONS*

BY

GORDON PALL

1. Some fifteen references, beginning with Euler, abstracted in Dickson's *History*,† use a connection between the congruence and equation

$$1) \qquad v_1^2 + v_2^2 + v_3^2 \equiv 0 \pmod{m}, \qquad t_0^2 + t_1^2 + t_2^2 + t_3^2 = m,$$

in the case where m is a prime, to prove that every positive integer is a sum of four squares. This connection is made precise, for arbitrary odd m, in Theorem 4. Among our theorems will be found conditions for quaternions to have the same right or left divisors of given norms. An easy derivation of known relations concerning binary quadratic class-numbers and representation in $x_1^2+x_2^2+x_3^2$ concludes the article.

Most of these results were discovered during an investigation of the "rational automorphs of $x_1^2+x_2^2+x_3^2$," and many of them are used in an associated article of that name. Since these automorphs are connected more simply with Lipschitz quaternions than with those of Hurwitz in which the coordinates may be halves of odds, our results are stated for the former type of integral quaternion, although there is no difficulty in extending them to the latter. No further mention is made in this article of automorphs.‡

Notations. The letters $a, b, c, t, u, \cdots, z$ denote integral quaternions of the type $t=t_0+i_1t_1+i_2t_2+i_3t_3$, with rational integer coordinates t_i. Conjugate and norm are defined as usual: $\bar{t}=t_0-\sum i_\alpha t_\alpha$, $Nt=\bar{t}t=\sum t_i^2$. Except for the quaternion units i_α, letters with subscripts, and $d, e, \cdots, s$ denote rational integers; p denotes an odd prime, *m an odd positive integer*. Subscripts α or β range over 1, 2, 3; i, j, f, or g over 0, 1, 2, 3.

We call t *pure* (mod m) if $m \mid t_0$; *proper* (mod m) if the g.c.d. of $t_0, \cdots, t_3$, and m is 1; *proper* if the g.c.d. of $t_0, \cdots, t_3$ is 1.

German capitals represent the sets defined as follows:

---

* Presented to the Society in part April 15, 1933, under the title *On the relations between sums of three and four squares*, and in part April 13, 1940; received by the editors January 31, 1940. This paper was received by the editors of the Annals of Mathematics July 5, 1939, accepted by them, and later transferred to these Transactions.

† L. E. Dickson, *History of the Theory of Numbers*, vol. 2, chap. 8.

‡ The complications of Lipschitz's article are partly due to their use. (R. Lipschitz, Journal de Mathématique, (4), vol. 2 (1886), pp. 373–439.) Several papers by the writer, now published, owe their inception to the study of the rational automorphs, and some of their proofs now stated in terms of quaternions were originally obtained by automorphs. The associated article mentioned above will appear soon in the Annals of Mathematics.

$\mathfrak{Q}$: eight left-associate proper quaternions $\pm t$, $\pm i_\alpha t$;

$\mathfrak{E}$: the set obtained from a given proper quaternion t by an even number of sign-changes or interchanges of the coordinates t_i;

$\mathfrak{M}$: m pure quaternions of norm zero, and proportional, (mod m); that is $0, v, 2v, \cdots, (m-1)v$ (mod m), where v is pure and proper (mod m), $m \mid Nv$.

2. If t is a right divisor of x, that is, $x = ut$ in integral quaternions, then the left-associates $\pm t$, $\pm i_\alpha t$ are right divisors of x with the same norm.

THEOREM 1. *If $v = v_0 + i_1 v_1 + i_2 v_2 + i_3 v_3$ is proper* (mod m), $m \mid Nv$, *m odd and positive, then v has precisely one set $\mathfrak{Q}$ of right divisors of norm m.*

This theorem, fundamental in the arithmetic of quaternions, was proved by Lipschitz* in the case of a prime m by a modification of Euler's method of proof that every prime is a sum of four squares. Hermite† had an elegant device for proving the four square theorem, based on the fact that there is only one class of positive quaternary quadratic forms of determinant 1. The following proof of Theorem 1 is an adaptation of Hermite's method. An extension of this proof to generalized quaternions has already been published.‡

LEMMA 1. *If $x \equiv y$* (mod m), *x and y have the same right divisors of norm m.*

For if $v = ut$ and $Nt = m$, $v + zm = (u + z\bar{t})t$.

LEMMA 2. *If Nx is prime to m, v and xv have the same right divisors of norm m.*

For if $v = ut$, $xv = (xu)t$. Conversely if $xv = ut$, choose k so that $kNx \equiv 1$ (mod m); *then* $v \equiv (k\bar{x}u)t$ (mod m), and we apply Lemma 1.

LEMMA 3. *If Theorem 1 holds for every product m of $r-1$ primes or less ($r > 1$), it holds for products m of r primes.*

See the top ten lines on page 702 of the reference just cited.

LEMMA 4. *If v is proper* (mod p), *we can choose a pure quaternion x of norm prime to p, such that xv is pure* (mod p).

We assume as we may that $p \nmid v_1$, and must choose x to satisfy

$$x_1 v_1 + x_2 v_2 + x_3 v_3 \equiv 0, \qquad x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \pmod{p}. \tag{2}$$

Solving (2_1) in the form $x_1 \equiv e x_2 + f x_3$, we reduce (2_2) to

$$(1 + e^2)x_2^2 + 2ef x_2 x_3 + (1 + f^2)x_3^2 \not\equiv 0 \pmod{p}.$$

* Loc. cit., pp. 416–420.

† C. Hermite, Journal für die reine und angewandte Mathematik, vol. 47 (1854), pp. 343–345; *Oeuvres*, vol. 1, pp. 234–237.

‡ G. Pall, Duke Mathematical Journal, vol. 4 (1938), pp. 696–704.

Since these three coefficients are not all zero (mod p), Lemma 4 follows.

By these lemmas the proof of Theorem 1 reduces to the case where m is a prime p, and v is a pure quaternion such that

$$v = i_1 - i_2v_2 - i_3v_3, \qquad 1 + v_2^2 + v_3^2 = pq, \qquad q \text{ an integer.} \tag{3}$$

How many quaternions t satisfy $v=ut$, $Nt=p$, or what is equivalent:

$$v\bar{t} \equiv 0, \qquad Nt = p? \tag{4}$$

Condition (4_1) expands into four linear congruences in the t_i. In view of $1+v_2^2+v_3^2\equiv 0$ these reduce to the two congruences

$$t_0 \equiv v_3t_2 - v_2t_3, \qquad t_1 \equiv v_2t_2 + v_3t_3 \pmod{p}. \tag{5}$$

We therefore substitute in the condition $\sum t_i^2=p$ the expressions

$$t_0 = pX_0 + v_3X_2 - v_2X_3, \quad t_1 = pX_1 + v_2X_2 + v_3X_3, \quad t_2 = X_2, \quad t_3 = X_3, \tag{6}$$

where the X_i are integers, and, on dividing through by p, obtain

$$p(X_0^2 + X_1^2) + 2v_3(X_0X_1 + X_2X_3) - 2v_2(X_0X_3 - X_1X_2) + q(X_2^2 + X_3^2) = 1. \tag{7}$$

This form is positive, being derived from $\sum t_i^2$, and is of determinant $(p^2)^2/p^4=1$, hence equivalent to $\sum x_i^2$. Hence (7) has eight solutions $(X_0, \cdots, X_3)$. If t is any of the corresponding values (6), its left-associates exhaust the eight possibilities. Theorem 1 follows.

COROLLARY 1. *Theorem* 1 *holds with m even* [change of notation momentary], *provided v is actually proper and Nv/m is odd.*

For, if $v=ut$ and u is determined up to a right unit factor, then t is determined up to a left unit factor.

COROLLARY 1′. *If z and xz are both proper* (mod m), *and* $m \mid Nz$, *then z and xz have the same right divisors of norm m.*

3. We now consider the left-multiples of a proper quaternion t.

LEMMA 5. *Let t be proper,* $p \nmid t_0^2+t_\alpha^2$ *for some* α. *No two of the following* p^{2k} *quaternions are congruent* (mod p^k):

$$(e + fi_\alpha)t, \qquad e, f = 0, 1, \cdots, p^k - 1. \tag{8}$$

From $(r+si_\alpha)t\equiv 0 \pmod{p^k}$ follows $r\equiv s\equiv 0$, for

$$rt_0 - st_\alpha \equiv 0, \qquad rt_\alpha + st_0 \equiv 0, \qquad r(t_0^2 + t_\alpha^2) \equiv 0 \equiv s(t_0^2 + t_\alpha^2).$$

THEOREM 2. *Let t be proper,* $p^k \mid Nt$. *Then ut represents precisely* p^{2k} *residues* (mod p^k), *each residue for* p^{2k} *residues u* (mod p^k).

We cannot have $p \mid t_0^2+t_\alpha^2$ for $\alpha=1, 2$, and 3; for then $p \mid \sum(t_0^2+t_\alpha)=2t_0^2+Nt$, $p \mid t_i$ $(i=0, 1, 2, 3)$. Let κ denote the number of solutions x of $xt \equiv 0$, and ρ the number of residues $ut \pmod{p^k}$. The number of solutions x of $xt \equiv wt$, for a given w, is the same as that of $(x-w)t \equiv 0$, hence equals κ; that is, every residue ut is represented for κ residues u, whence $\kappa\rho = p^{4k}$. By Lemma 5, $\rho \geqq p^{2k}$; since $x=(e+fi_\alpha)\bar{t}$ obviously satisfies $xt \equiv 0$, $\kappa \geqq p^{2k}$. Hence $\kappa=\rho=p^{2k}$.

COROLLARY 2. *If $p^k \mid Nt$ the residues* (8) *in Lemma* 5 *represent a complete set of left-multiples of t,* (mod p^k).

COROLLARY 3. *In Theorem* 2 *precisely p^k of the p^{2k} left-multiples of t* (mod p^k) *are pure* (mod p^k).

THEOREM 3. *Let t be proper, $m \mid Nt$. Then all left-multiples ut* (mod m) *which are pure* (mod m) *form an unique set $\mathfrak{M}$; that is, all pure left-multiples of t are proportional* (mod m).

For, by Corollary 3 and the Chinese remainder theorem applied with $m=\prod p^r$, there are precisely m pure left-multiple residues $ut \pmod{m}$. At least one, say v, is proper, by Lemma 4. Then $0, v, 2v, \cdots, (m-1)v$ exhaust the m possibilities.

THEOREM 4. *To every set $\mathfrak{Q}$ of norm m corresponds one and only one set $\mathfrak{M}$* (mod m), *and conversely, such that $\mathfrak{M}$ contains the pure left-multiples* (mod m) *of the quaternions in $\mathfrak{Q}$, and $\mathfrak{Q}$ contains the right divisors of norm m of the proper elements of $\mathfrak{M}$.*

By taking conjugates we have a similar result for pure right-multiples and left divisors. Since the various left-multiple sets $\mathfrak{M} \pmod{p^r}$ of x and y are the same and combine, by the C.r.t., into an unique $\mathfrak{M} \pmod{m}$ we have

COROLLARY 4. *Let x and y be proper* (mod m), $Nx \equiv Ny \equiv 0$. *If x and y have the same right divisors of norm p^r, for every p^r dividing m, then x and y have the same right divisors of norm m.*

COROLLARY 5. *Let v be proper and pure* (mod m), $m \mid Nv$, *and let wv be pure* (mod m). *Then there exists an integer λ such that $wv \equiv \lambda v$.*

4. Conditions for quaternions to have the same divisors will be discussed.

LEMMA 6. *The largest rational integer factor of m dividing z is not changed if z is replaced by uz, or zu, where Nu is prime to m.*

For let $k \mid m$. If $k \mid z$, $k \mid uz$. If $k \mid uz$, $k \mid \bar{u}uz$, $k \mid z$.

LEMMA 7. *If $t', t'', \cdots, t^{(f)}$ are quaternions of odd prime norm p, then $t=t't'' \cdots t^{(f)}$ is proper if and only if*

$$t^{(g)}t^{(g+1)} \text{ is proper for } g = 1, 2, \cdots, f-1. \tag{9}$$

The lemma is trivial if $f=2$. The necessity of (9) is obvious for every f. Assume for a given f that (9) holds and t is proper. Consider $x=tt^{(f+1)}$. If x is not proper, $x=yp$, y integral; and since $p=\bar{t}^{(f+1)}t^{(f+1)}$, $t=y\bar{t}^{(f+1)}$. Hence $t^{(f)}=\theta\bar{t}^{(f+1)}$, since both are right divisors of t of norm p, θ denoting a unit ± 1 or $\pm i_\alpha$. Thus $t^{(f)}t^{(f+1)}=\theta p$.

By a similar argument we obtain

LEMMA 8. *Let $u', u'', \cdots, u^{(h)}$ be of norm p. If any $u^{(g)}u^{(g+1)}$ is improper, it is of the form θp, θ a unit; we can remove the factor p from $u=u'u''\cdots u^{(h)}$, absorb the unit θ into $u^{(g-1)}$ or $u^{(g+2)}$, and proceed with the remaining product of $h-2$ factors. We obtain finally $u=p^r t'\cdots t^{(f)}$, $t'\cdots t^{(f)}$ proper as in Lemma 7, $f=h-2r$.*

LEMMA 9. *If x and y are proper* (mod p), *and $xy\equiv 0$* (mod p^r), *then $p^r \mid Nx$ and Ny, and x and $\bar{y}$ have the same right divisors of norm p^r.*

For, if $p^r \mid xy$, $p^r \mid \bar{x}xy$ and $xy\bar{y}$, whence $p^r \mid Nx$ and Ny. Hence we can write $x=uu't$, $\bar{y}=\bar{v}\bar{v}'\bar{t}'$, where $Nt=Nt'=p^r$, $Nu'=p^e$, $Nv'=p^f$ $(e,\ f\geqq 0)$, and $p\nmid NuNv$. Then $xy=uu'tt'v'v\equiv 0$ (mod p^r), $u't$ and $t'v'$ being proper. By Lemmas 6 and 8, $tt'\equiv 0$ (mod p^r), that is, t and $\bar{t}'$ are left-associates.

THEOREM 5. *Let x and y be proper* (mod m). *Then x and y have the same right divisors of norm m, if and only if $x\bar{y}\equiv 0$* (mod m).

For if $x=ut$, $y=vt$, and $Nt=m$, then $x\bar{y}=ut\bar{t}\bar{v}=mu\bar{v}\equiv 0$. Conversely, if $x\bar{y}\equiv 0$, we apply Lemma 9 and Corollary 4.

THEOREM 6. *Let x and y be proper* (mod m), *$m \mid Nx$ and Ny. Then there exists a factorization $m=m_1m_2$ in odd positive integers, such that x and y have the same left divisors of norm m_1 and the same right divisors of norm m_2, if and only if*

$$m \mid (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3). \tag{10}$$

Necessity. If t' and t'' are left and right divisors of x, of norms m_1 and m_2 respectively, then $x=ut''$ where $m_1 \mid Nu$, and the left divisor of norm m_1 of u must be t' (by the uniqueness feature of Theorem 1). Hence we can set $x=t'at''$, $y=t'bt''$, $Nt'=m_1$, $Nt''=m_2$. The expression in (10) is

$$\begin{aligned}\tfrac{1}{2}(x\bar{y}+y\bar{x}) &= \tfrac{1}{2}(t'at''\bar{t}''\bar{b}\bar{t}' + t'bt''\bar{t}''\bar{a}\bar{t}')\\ &= \tfrac{1}{2}Nt''(t'a\bar{b}\bar{t}' + t'b\bar{a}\bar{t}') = \tfrac{1}{2}Nt''[t'(a\bar{b}+b\bar{a})\bar{t}']\\ &= \tfrac{1}{2}Nt''(a\bar{b}+b\bar{a})Nt' = m_1m_2\sum a_ib_i,\end{aligned}$$

Nt'' and $a\bar{b}+b\bar{a}$ being scalars.

Sufficiency. From $x\bar{y}+y\bar{x}\equiv 0$ and $\bar{x}x\equiv 0$ follow

$$x\bar{y}x + y\bar{x}x \equiv 0, \qquad x\bar{y}x \equiv 0 \pmod{m}.$$

Let p^r be any prime-power dividing m. Then $p^r \mid x\bar{y}x$. Let p^s be the highest power of p for which $p^s \mid x\bar{y}$. By Theorem 5, x and y have the same right divisor of norm p^s. If $s \geqq r$ this result suffices as regards p. If $r > s$, we can set $x = ut$, $y = vt$, $Nt = p^s$, whence $u\bar{v}$ is proper and $p^{r-s} \mid Nv$. Then $p^{r-s} \mid u\bar{v}x$. Hence by Theorem 5, $v\bar{u}$ and x have the same left divisors of norm p^{r-s}. These must coincide with the left divisors of v with norm p^{r-s}, and hence with those of y. Corollary 4 now gives us Theorem 6.

The expansion of $x\bar{y} \equiv 0 \pmod{p^r}$ is as follows:

$$x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 \equiv 0 \pmod{p^r}, \tag{11}$$

$$\begin{cases} (x_0y_1 - x_1y_0) + (x_2y_3 - x_3y_2) \equiv 0 \pmod{p^r}, \\ (x_0y_2 - x_2y_0) + (x_3y_1 - x_1y_3) \equiv 0 \pmod{p^r}, \\ (x_0y_3 - x_3y_0) + (x_1y_2 - x_2y_1) \equiv 0 \pmod{p^r}. \end{cases} \tag{12}$$

THEOREM 5′. *Let $m \mid Ny$, y proper* (mod m). *Then the right divisors of y with norm m are right divisors of x, if and only if, for each prime-power p^r dividing m,* (11) *holds along with* (12_α), *where α ($=1$, 2, or 3) is such that $p \nmid y_0^2 + y_\alpha^2$. Similarly for left divisors with the $+$'s in* (12) *changed to $-$'s.*

Note that $p \nmid y_0^2 + y_\alpha^2$ for $\alpha = 1$, 2, or 3, since $p \mid Ny$ but $p \nmid y$.

We may assume $\alpha = 1$. Since $p^r \mid Ny$ we readily verify that

$$(-y_0y_2 + y_1y_3)(11) - (y_0y_3 + y_1y_2)(12_1) + (y_0^2 + y_1^2)(12_2) \equiv 0,$$
$$-(y_0y_3 + y_1y_2)(11) + (y_0y_2 - y_1y_3)(12_1) + (y_0^2 + y_1^2)(12_3) \equiv 0.$$

Hence (11)–(12_α) imply (12), and the four congruences (11)–(12) have p^{2r} solutions x (mod p^r), m^2 solutions x (mod m). But by Theorem 2, if $y = vt$, $Nt = m$, then $x = ut$ has m^2 residues (mod m). Every such residue satisfies $x\bar{y} \equiv 0$. Incidentally, this gives an alternative proof of Theorem 5.

COROLLARY 6. *Let x be pure and proper* (mod m), $d^2 + Nx \equiv 0 \equiv e^2 + Nx$. *Then $d + x$ and $e + x$ have the same right divisors of norm m if and only if $d \equiv e$.*

COROLLARY 7. *If x is pure, and v is pure and proper* (mod m), $m \mid Nv$ *and* $m \mid \sum x_\alpha v_\alpha$, *then there exists an integer x_0 such that $x_0 + x$ and v have the same right divisors of norm m.*

For we have only to choose x_0 to satisfy any one of

$$x_0v_1 + x_2v_3 - x_3v_2 \equiv 0, \quad x_0v_2 + x_3v_1 - x_1v_3 \equiv 0, \quad x_0v_3 + x_1v_2 - x_2v_1 \equiv 0 \ (p^r),$$

in which $p \nmid v_\alpha$, for each prime-power dividing m.

COROLLARY 8. *If y is proper* (mod m), *and $m \mid Ny$, then x has the right divisors of norm m of y, and the left divisors of norm m of y, if and only if $x \equiv ky$* (mod m) *for some integer k.*

For then $x_f y_g - x_g y_f \equiv 0 \pmod{p^r}$, $f, g = 0, 1, 2, 3$.

The value of k may sometimes be obtained from the identity

$$tat = 2(a_0 t_0 - \sum a_\alpha t_\alpha)t - \bar{a} N t.$$

COROLLARY 9. *If $m \mid Nx$, Ny, and $\sum x_i y_i$, and x and y are proper* (mod m), *then there is a factorization $m = m_1 m_2$ such that*

$$(x_0 y_1 - x_1 y_0) \equiv \pm (x_2 y_3 - x_3 y_2), \qquad (x_0 y_2 - x_2 y_0) \equiv \pm (x_3 y_1 - x_1 y_3),$$
$$(x_0 y_3 - x_3 y_0) \equiv \pm (x_1 y_2 - x_2 y_1),$$

with all the signs $\pm$ taken as $+$ for modulus m_1, and $-$ for modulus m_2.

COROLLARY 10. *If m has no square factor greater than* 1, *x and y are pure and proper, $m \mid Nx$, Ny, and $\sum x_\alpha y_\alpha$, then x and y are proportional* (mod m).

The most interesting special case of Theorem 6 is

THEOREM 7. *Let x and y be proper* (mod p), *p an odd prime dividing Nx and Ny. Then x and y have either the same right divisors or the same left divisors, or both, of norm p, if and only if*

$$x_0 y_0 + x_1 y_1 + x_2 y_2 + x_3 y_3 \equiv 0 \pmod{p}. \tag{13}$$

An independent proof involves interesting lemmas:

LEMMA 10. *If $Nt = p$, p cannot divide two of $t_0^2 + t_\alpha^2$ ($\alpha = 1, 2, 3$).*

For if $p \mid t_0^2 + t_\alpha^2 \leqq p$, then $t_0^2 + t_\alpha^2 = p$.

LEMMA 11. *If $Nt = p = Nt'$, then exactly p of the p^2 left-multiples of t,* (mod p), *are also right-multiples of t'.*

For by Lemma 10 we can assume $p \nmid t_0^2 + t_1^2$ and $p \nmid t_0'^2 + t_1'^2$. By Theorem 5′, t' and $(e + f i_1)t$ (cf. Lemma 5) have the same left divisors of norm p if and only if, to modulus p,

$$e(t_0 t_0' + t_1 t_1' + t_2 t_2' + t_3 t_3') + f(t_0 t_1' - t_1 t_0' + t_2 t_3' - t_3 t_2') \equiv 0,$$
$$e(t_0 t_1' - t_1 t_0' - t_2 t_3' + t_3 t_2') + f(-t_0 t_0' - t_1 t_1' + t_2 t_2' + t_3 t_3') \equiv 0.$$

The determinant is easily seen to be zero (mod p) while not all the coefficients are zero. Hence there are p solutions e, f.

LEMMA 12. *For a given y such that $p \nmid y$ but $p \mid Ny$, there are precisely $2p^2 - p$ solutions x_0, x_1, x_2, x_3 of*

$$(14)\qquad y_0x_0 + y_1x_1 + y_2x_2 + y_3x_3 \equiv 0, \qquad x_0^2 + x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{p}.$$

Although a direct proof is not difficult, we deduce this from a general investigation of such congruences.*

The solutions x of (14) must coincide with the $2p^2-p$ residues having the same right or left divisors of norm p as y, since those residues satisfy (14).

5. Including the original t, there are twenty-four (not necessarily distinct) values $t_0 \pm i_1t_\alpha \pm i_2t_\beta \pm i_3t_\gamma$ in a set $\mathfrak{E}$, obtained by an even number of interchanges and sign-changes of t_1, t_2, t_3. In this way we find a value t in every subset $\mathfrak{Q}$ of $\mathfrak{E}$. We can easily verify

LEMMA 13. *The twenty-four notationally distinct elements in a set $\mathfrak{E}$, with fixed t_0, can be expressed by*

$$\eta t\bar{\eta},$$

$$(15)\qquad \eta = 1,\ i_\alpha,\ (1 + i_\alpha)/2^{1/2},\ (1 - i_\alpha)/2^{1/2},\ (i_\alpha - i_{\alpha+1})/2^{1/2},\ (i_\alpha + i_{\alpha+1})/2^{1/2},$$

$$\tfrac{1}{2}(1 + i_1 + i_2 + i_3) = \nu,\ i_\alpha\nu,\ \bar{\nu},\ \bar{\nu}i_\alpha,$$

where $\alpha = 1, 2, 3$, and $i_4 = i_1$.

Consider the relation between divisors of elements x and x' in the same set $\mathfrak{E}$. We choose the left-associate of x' having the same real part as x. This left-associate has the same right divisors as x', and is of the form $\eta x\bar{\eta}$, as in (15). From $x = ut$ follows

$$(16)\qquad \eta x\bar{\eta} = \eta u\bar{\eta}\cdot\eta t\bar{\eta}.$$

This is also evident from the fact that an even number of interchanges and sign-changes of i_1, i_2, i_3 produces a simply isomorphic system of quaternions.

The factorization of the quaternions obtained from x by an odd number of permutations and sign-changes of the x_i reduces similarly to that of $\bar{x}$. Trivially, $x = ut$ implies $\bar{x} = \bar{t}\bar{u}$. But the right divisors of x and $\bar{x}$ are not related in any obvious way. Some light on this question is exhibited by

THEOREM 8. *Let x be proper* (mod m), $m \mid Nx$. *Then x and $\bar{x}$ have their right divisors of norm m in the same set $\mathfrak{E}$ if and only if*

$$(17)\qquad m \text{ divides one of } x_f,\ x_f \pm x_g\ (f \neq g),\ x_0 \pm x_1 \pm x_2 \pm x_3.$$

Set $\theta = e\bar{\eta}$, η as in (15), with $e = 1, 2^{1/2}$, or 2 in the respective cases, so that θ is integral, proper, and of norm e^2. Consider

$$(18)\qquad 2s_0 = x\theta + \bar{\theta}\bar{x}, \qquad s_0 \text{ the scalar part of } x\theta.$$

* R. E. O'Connor, *Quadratic and linear congruence*, Bulletin of the American Mathematical Society, vol. 45 (1939), pp. 792–798.

The values of s_0 are precisely the expressions in (17), or their negatives. Let $x=ut$, $Nt=m$. We shall see that

(19) $\bar{x}$ has the right divisor $t' = \eta t\bar{\eta}$, if and only if $m \mid s_0$.

From (18) we obtain

(20) $$e^2\bar{x} = 2\theta s_0 - \theta x\theta = 2\theta s_0 - \theta u\theta\eta t\bar{\eta} = 2\theta s_0 - u't'.$$

If $\bar{x}=vt'$, then $2e^2s_0=yt'$, $m=Nt' \mid 2e^2s_0\bar{t}'$, hence $m \mid s_0$. Conversely, if $m \mid s_0$, $t'=\eta t\bar{\eta}$ is a right divisor of $2\theta s_0$, hence by (20) of $e^2\bar{x}$, hence of $\bar{x}$ (e^2 being prime to m).

THEOREM 9. *Let t be proper, $Nt=m$. Let $\mathfrak{M}_1$ and $\mathfrak{M}_2$ denote, respectively, the set of pure left- and right-multiples of t* (mod m). *Then $\mathfrak{M}_1$ and $\mathfrak{M}_2$ can be obtained from each other by interchanges or sign-changes of i_1, i_2, i_3, if and only if*

(21) *two of t_0^2, t_1^2, t_2^2, t_2^3, 0 are equal.*

Necessity. Let $v=at$, $v'=tb$, where v and v' are pure (mod m), and v' is obtained from v by permuting or changing signs of v_1, v_2, v_3. Then $\pm v'=\eta v\bar{\eta}$ $=\eta a\bar{\eta}\cdot\eta t\bar{\eta}$, while $-v'=\bar{v}'=\bar{b}\bar{t}$. Since v' is pure, (17) holds trivially with $v=x$, so that $\bar{t}$ and $\eta t\bar{\eta}$ are in the same $\mathfrak{E}$, whence (21).

Sufficiency. If (21) holds, $\bar{t}$ and t are in the same $\mathfrak{E}$. By (16), the left-multiples of t are obtained from those of $\bar{t}$ by permuting and changing signs of i_1, i_2, i_3. The pure left-multiples of $\bar{t}$ are right-multiples of t.

6. Let $h(-n)$ denote the number of classes of primitive, positive, binary quadratic forms $\phi=[k, 2x_0, l]$ of determinant $-n=x_0^2-kl$, and $r'(n)$ the number of proper pure quaternions x of norm n. Gauss showed that, if $n>1$, $n\neq 4f$ or $8f+7$,

(22) $$\begin{aligned} r'(n) &= 12h(-n), \quad \text{if} \quad n \equiv 1 \text{ or } 2 \pmod 4, \\ &= 8h(-n), \quad \text{if} \quad n \equiv 3 \pmod 8. \end{aligned}$$

Assuming that $r'(n)>0$ we demonstrate (22) by means of quaternions.

Let $[x]$ denote the set of four quaternions

(23) $$x, \quad -i_1xi_1 = i_1x_1 - i_2x_2 - i_3x_3, \quad -i_2xi_2, \quad -i_3xi_3,$$

obtained by changing signs of two x_α; four, that is, except for $Nx=1$, when only two of them are distinct. With ϕ we associate the following *process* whereby: (a) *every proper $[x]$ of norm n is carried into a certain proper $[y]$ of norm n*; (b) *no two distinct proper $[x]$'s are carried into the same $[y]$*.

Set $x_0+x=ut$, $Nu=l$, $Nt=k$, which confines t to a set $\mathfrak{Q}$ (Corollary 1). Define $y=(tx\bar{t})/k=tu-x_0$. If t is replaced by a left-associate $i_\beta t$, y is replaced

by $-i_\beta y i_\beta$, in $[y]$. If t is changed to $-t$, y is unaltered. If x is replaced by $x' = -i_\alpha x i_\alpha$, $x_0 + x' = -i_\alpha u t i_\alpha$, and we again obtain y.

Further, y is proper. For if $p \mid y$, then $p \mid n = Ny$; and $p \mid k$, since $kx = \bar{t}yt$ and x is proper. Since $x_0^2 + n = kl$, $p \mid x_0$. Hence $p \mid tu = y + x_0$. Since t is proper, $p \mid tNu$, $p \mid Nu = l$, contradicting the primitivity of $[k, 2x_0, l]$.

Reciprocally, since $\bar{y} = -y$, $-x_0 + y = -\bar{u}\bar{t}$, whence $\bar{t}yt = kx$, and the process associated with $[k, -2x_0, l]$ carries $[y]$ back into $[x]$; hence (b).

LEMMA 14. *The process associated with the primitive form $\phi = [k, 2x_0, l]$ is the same as that for the following forms equivalent to ϕ:*

$$[k, 2(x_0 + hk), \cdots], \qquad [l, -2x_0, k]. \tag{24}$$

For, if $x_0 + x = ut$, then $x_0 + hk + x = (u + h\bar{t})t$; and $-x_0 + x = -\bar{t}\bar{u}$, $(\bar{u}xu)/l = y = tu - x_0$, since $\bar{y} = -y$.

COROLLARY 11. *Any two equivalent forms ϕ determine the same process.*

LEMMA 15. *Let C, D denote primitive, positive classes of determinant $-n$, CD the product-class under composition. If C carries the proper $[x]$ into $[y]$, and D carries $[y]$ into $[z]$, then CD carries $[x]$ into $[z]$.*

We can choose representative forms in the classes C and D of the types $\phi = [k, 2x_0, hl]$, $\psi = [h, 2x_0, kl]$. By assumption,

$$\begin{aligned} x_0 + x &= ut, \qquad Nt = k, \qquad (tx\bar{t})/k = y = tu - x_0, \\ x_0 + y &= vt', \qquad Nt' = h, \qquad (t'y\bar{t}')/h = z = t'v - x_0. \end{aligned}$$

Hence $tu = vt'$; since $Nu = hl$, $u = wt'$,

$$x_0 + x = w(t't), \qquad N(t't) = hk, \qquad (t'tx\bar{t}\bar{t}')/(hk) = z.$$

By $\mathfrak{R} = \mathfrak{R}(y)$ we mean the set of pure quaternions obtained from a pure y by permuting and changing signs of y_1, y_2, y_3.

LEMMA 16. *If $Nv = 2^r$, then $(\bar{v}yv)/Nv$ is in $\mathfrak{R}(y)$.*

For v is a product of factors $\pm i_\alpha$, $1 + i_\beta$. Now $-i_\alpha y i_\alpha$ is in $[y]$; and $(1 + i_1)y(1 - i_1) = 2(i_1 y_1 - i_2 y_3 + i_3 y_2)$.

LEMMA 17. *If x and y are pure and proper, and $Nx = Ny$, there exists a proper quaternion t of odd norm m such that, for some y' in $\mathfrak{R}(y)$,*

$$txt' = my'. \tag{25}$$

For, $x^2 = y^2$, $(x+y)x = y(x+y)$, $(x+y)x(\overline{x+y}) = yN(x+y)$. If $y = -x$, the theorem is trivial: $y' = x$, $t = 1$. Hence we can suppose $x + y \neq 0$, $x + y = vt$, Nv a power of 2, Nt odd; $tx\bar{t} = m(\bar{v}yv/Nv)$.

If a proper $[x]$ can be carried into $[y]$ by the process associated with a

primitive class C, then $tx\bar{t}=(Nt)y$ must be solvable with t proper and Nt prime to any assignable number. For C contains such forms $[Nt, 2x_0, l]$.

LEMMA 18. *If x is pure, t proper, and $Nt=m$ odd, and if $tx\bar{t}=my$, then we can find an integer x_0 such that $x_0+x=ut$ (whence $y=tu-x_0$).*

For $tx=yt$ has the right and left divisors of norm m of t. By Corollary 8, $tx\equiv x_0 t \pmod m$ for some integer x_0. Hence

$$(x_0+x)\bar{t}=x_0\bar{t}-\bar{x}\bar{t}\equiv x_0\bar{t}-x_0\bar{t}\equiv 0,\quad (x_0+x)\bar{t}=mu,\quad x_0+x=ut.$$

LEMMA 19. *There is at most one primitive class of determinant $-n$ carrying any given proper $[x]$ of norm n into any given proper $[y]$ of norm n.*

For if C and D carry $[x]$ into $[y]$, then both $F=CD^{-1}$ and the principal class E carry $[x]$ into $[x]$. From $tx\bar{t}=mx$, $Nt=m$, follows $tx=xt$, or

$$x_2t_3=x_3t_2,\qquad x_3t_1=x_1t_3,\qquad x_1t_2=x_2t_1.$$

Since x is proper, $t_\alpha=gx_\alpha$ for some integer g, $(\alpha=1, 2, 3)$. The condition $Nt=m$ becomes $t_0^2+ng^2=m$. Thus E represents every integer represented properly by F, $E\sim F$.

LEMMA 20. *Let x' be obtained from x by r sign-changes and s interchanges of x_1, x_2, x_3. Then a proper quaternion t of odd norm such that*

$$tx\bar{t}=(Nt)x' \tag{26}$$

exists if and only if: (α) $x'\equiv x$ (2), (β) *r is even if* $Nx\equiv 3$ (8).

On expanding $tx\bar{t}$ we find $tx\bar{t}\equiv(Nt)x \pmod 2$, whence (α) is necessary. To prove the necessity of (β) we have to prove the impossiblity of $tx\bar{t}=-mx$ with Nt odd, that is, of $tx=-xt$, Nt odd, x_1, x_2, x_3 odd. Expanded, these imply

$$x_1t_1+x_2t_2+x_3t_3=0,\qquad x_1t_0=x_2t_0=x_3t_0=0,$$

whence $t_0=0$, $t_1+t_2+t_3$ is even, Nt is even.

Conversely it suffices to exhibit a solution t of (26) in the cases

$$(\gamma)\ x'=-x,\ Nx\equiv 1 \text{ or } 2 \pmod 4;\quad (\delta)\ x'=i_1x_2+i_2x_1+i_3x_3,\ x_1\equiv x_2\,(2).$$

For (γ), $(x_2i_3-x_3i_2)x(x_3i_2-x_2i_3)=(x_2^2+x_3^2)(-x)$ suffices, since one of $x_2^2+x_3^2$, $x_3^2+x_1^2$ is odd. For (δ), $t=(x_1+x_2)(i_1+i_2)/2+i_3x_3$ is effective, and is of odd norm unless $n\equiv 2 \pmod 4$, in which case $0+x=-(i_1+i_2)t$, where $\bar{u}=i_1+i_2$ (and hence t by Lemma 14) carries x into $i_1x_2+i_2x_1-i_3x_3$, and the sign-change is seen to in (γ). By (α) and (β) we have

COROLLARY 12. *If $Nx\equiv 1$ or 2 (mod 4), x can be transformed into precisely one-third of the vectors in $\mathfrak{R}(x)$. If $Nx\equiv 3 \pmod 8$, x can be transformed into precisely half the vectors in $\mathfrak{R}(x)$.*

Hence the number of primitive classes C is, respectively, one-third and one-half of the number of proper sets $[x]$, and (22) follows.

7. The relations between the representations of n and p^2n as a sum of three squares are easily derived by quaternions.

LEMMA 21. *Every proper, pure y of norm p^2n is of the form $\bar{\imath}x\imath$, where $Nt=p$ and $Nx=n$. Here t and x are unique except that they may be replaced by θt and $\theta x\bar{\theta}$, where $\theta=\pm 1$ or $\pm i_\alpha$. If y is changed to $-i_\beta y i_\beta$, we still obtain the same values x. In this way every proper $[y]$ of norm p^2n is derived from an unique proper $[x]$ of norm n.*

For, by Theorem 1, $y=vt$ with $Nt=p$ and t in an unique $\mathfrak{Q}$. Here $p \mid Nv$, whence v has the same left divisors of norm p as $y=-\bar{y}=\bar{\imath}\bar{v}$. Hence $v=\bar{\imath}x$, and so on. That x is proper follows from $y=\bar{\imath}x\imath$, y proper.

However, a given proper $[x]$ of norm n gives rise to $p-(-n \mid p)$ proper sets $[y]$ of norm p^2n, since there are $p+1$ sets $\mathfrak{Q}$ of norm p and $1+(-n \mid p)$ of them make $\bar{\imath}x\imath \equiv 0 \pmod{p}$. The latter values t (by Lemma 18) are the left divisors of x_0+x, where $x_0^2+n\equiv 0 \pmod{p}$. If t and t' are not in the same $\mathfrak{Q}$, $\bar{\imath}x\imath$ and $\bar{\imath}'x\imath'$ are not in the same $[y]$, by the uniqueness feature of Lemma 21. Hence we have

$$r'(p^2n) = \{p - (-n \mid p)\}r'(n). \tag{27}$$

Using "proper (mod p)" in place of "proper," we obtain

$$r''(p^2n) = \{p - (-n \mid p)\}r''(n),$$

where $r''(n)$ denotes the number of representations of n as a sum of three squares not all divisible by p. Let $r(n)$ denote the total number of representations of n as a sum of three squares. Then

$$\begin{aligned} r(p^2n) &= r(n) + r''(p^2n) = r(n) + \{p - (-n \mid p)\}r''(n) \\ &= r(n) + \{p - (-n \mid p)\}\{r(n) - r(n/p^2)\}, \end{aligned}$$

that is,

$$r(p^2n) = [p + 1 - (-n \mid p)]r(n) - [p - (-n \mid p)]r(n/p^2), \tag{28}$$

for any positive integer n. From this we readily deduce by induction that if h is quadratfrei and $m=\prod p_i^{\alpha_i}$ in powers of distinct primes,

$$\begin{aligned} r(m^2h) &= r(h)\cdot \prod \psi(p_i, \alpha_i; h), \\ \psi(p, \alpha; h) &= \frac{p^{\alpha+1}-1}{p-1} - (-h \mid p)\frac{p^\alpha - 1}{p-1}. \end{aligned} \tag{29}$$

Also, $r'(m^2h)=r'(h)\cdot\prod\phi(p_i, \alpha_i; h)$, where $\phi(p, \alpha; h)=p^\alpha-(-h \mid p)p^{\alpha-1}$.

8. Let h have no square factor greater than 1, m odd and positive. We shall prove that *the general solution of*

$$hm^2 = y_1^2 + y_2^2 + y_3^2 \tag{30}$$

in integers y_α *such that, if* $p \mid y = i_1y_1 + i_2y_2 + i_3y_3$, *then*

$$(-h \mid p) = 1, \quad \text{or} \quad p \mid h \quad \text{and} \quad p^2 \nmid y, \tag{31}$$

is given by $y = txi$, *where*

$$t \text{ is proper and } Nt = m, \ x \text{ is pure and } Nx = h. \tag{32}$$

If $y = txi$, $Ny = Nx(Nt)^2$, whence if (32) holds, y satisfies (30). To see that y also satisfies (31), set $y = p^e z = txi$. Then $p^{2e} \mid Ny = m^2h$, $p^e \mid m = p^e m'$. Hence $txm = p^e zt$, $txm' = zt \equiv \lambda t \pmod{m}$ for some integer λ by Corollary 8, $m' \mid \lambda = x_0 m'$ since t is proper, $tx \equiv tx_0 \pmod{p^e}$, $p^e \mid t(x_0 - x)(x_0 + x)$, $p^e \mid x_0^2 + h$; $(-h \mid p) = 1$, or $p \mid h$ and $e = 1$.

Conversely we have only to see that every solution y of (30) and (31) is of the required form txi. To do this we write $m = p^r m'$, $r > 0$, $p \nmid m'$, and show that $y = t'zi'$, t' proper of norm p^r, z pure and of norm hm'^2; then no prime p dividing z can satisfy $(-h \mid p) = -1$, or $p \mid h$ and $p^2 \mid z$, since such a prime divides $y = t'zi'$ and contradicts (31). Eliminating in turn each prime-power in m we finally obtain $y = txi$, with $t = t' \cdots t^{(k)}$ proper since the norms of $t', t'', \cdots$ are coprime in pairs. The proof of Lemma 21 extends to

LEMMA 22. *Let* u *be pure,* $p^{2s} \mid Nu$, u *proper* (mod p). *Then* $u = tvi$, t *proper,* $Nt = p^s$, $Nv = (Nu)/p^{2s}$.

Case $p \mid y$, $p \mid h$. By (31), $p^2 \nmid y$. Set $y = pu$, $m = pm_0$, $Nu = km_0^2$. Since u is proper (mod p) and $p^{2r-1} \mid Nu$, $u = tvi$, t proper, $Nt = p^{r-1}$, $Nv = km'^2$. Since $p \mid Nv$, $v = t'w$, $Nt' = p$, and hence $pv = t'v'i'$, where $v' = wt'$. Hence $y = pu = (tt')v'(i'i)$. Here tt' must be proper, since tv (a factor of u) is proper (mod p).

Case $p \mid y$, $(-h \mid p) = 1$. *Set* $y = p^e u$, u proper (mod p), $m = p^e m_0$, $Nu = hm_0^2$. Then $u = tvi$, $Nt = p^{r-e}$, $Nv = hm'^2$. There are two solutions $\pm v_0$ of $v_0^2 \equiv -hm'^2$ (mod p^e). Since $p \nmid v_0$, the left divisors of norm p of $v_0 + v$ and $-v_0 + v$ cannot be the same. Hence we can set $v_0 + v = t'w$, $Nt' = p^e$, t' proper, and choose the sign of v_0 to make tt' proper (Lemma 7). Then $v' = wt' - v_0 = (i'vt')/p^e$, and $p^e v = t'v'i'$, $y = (tt')v'(i'i)$.

Case $p \nmid y$. Then Lemma 22 applies at once.

The restriction that h be quadratfrei can be removed, if the troublesome case where $p^2 \mid h$ and $p^2 \mid y$ is avoided by reducing to h/p^2 and y/p.

9. As an addition to §6 we record the following results which depend only on n and not on the particular x of norm n:

(a) $[1, 0, n]$ carries x into x;

(b) $[2, 2, (n+1)/2]$ carries x into $(x_1, x_3, -x_2)$ if $n \equiv 1 \pmod 4$, $x_2 \equiv x_3 \ (2)$;

(c) $[2, 0, n/2]$ carries x into $(x_1, x_3, -x_2)$ if $n \equiv 2 \pmod 4$, $x_2 \equiv x_3 \ (2)$;

(d) $[4, 2, (n+1)/4]$ carries x into (x_2, x_3, x_1) or (x_3, x_1, x_2) if $n \equiv 3 \ (8)$, depending on the residue of $x_1+x_2+x_3 \pmod 4$, while for the same case,

(e) $[4, -2, (n+1)/4]$ carries x into the other of (x_2, x_3, x_1), (x_3, x_1, x_2).

McGill University,
Montreal, Quebec