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

\[ v_1^2 + v_2^2 + v_3^2 = 0 \pmod{m}, \quad t_0^2 + t_1^2 + t_2^2 + t_3^2 = m, \]

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 \( a, b, c, t, u, \ldots, z \) denote integral quaternions of the type \( t = t_0 + it_1 + it_2 + it_3 \), with rational integer coordinates \( t \). Conjugate and norm are defined as usual: \( \bar{t} = t_0 - \sum t_d d, \quad Nt = \bar{t}t = \sum t_d^2 \). Except for the quaternion units \( i, j, k \), letters with subscripts, and \( d, e, \ldots, s \) denote rational integers; \( p \) denotes an odd prime, \( m \) an odd positive integer. Subscripts \( \alpha \) or \( \beta \) range over \( 1, 2, 3; i, j, k, \) or \( g \) over \( 0, 1, 2, 3 \).

We call \( t \) pure \( \pmod{m} \) if \( m \mid t_0 \); proper \( \pmod{m} \) if the g.c.d. of \( t_0, \ldots, t_4 \), and \( m \) is 1; proper if the g.c.d. of \( t_0, \ldots, t_4 \) 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.
‡ 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.

487
Ω: eight left-associate proper quaternions \( \pm t, \pm i, \pm j, \pm k \);

Ω: the set obtained from a given proper quaternion \( t \) by an even number of sign-changes or interchanges of the coordinates \( t_i \);

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

2. If \( t \) is a right divisor of \( x \), that is, \( x = ut \) in integral quaternions, then the left-associates \( \pm t, \pm i, \pm j, \pm k \) are right divisors of \( x \) with the same norm.

**Theorem 1.** If \( v = v_0 + iv_1 + jv_2 + kv_3 \) is proper \((\text{mod } m), m \mid Nv, m \text{ odd and positive} \), then \( v \) has precisely one set \( \mathcal{Q} \) 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 \( Nt = m, v + zm = (u + zi)t \).

**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 \( kNx = 1 \mod m \); then \( v = (kxu)t \mod m \), 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 \((\text{mod } p) \), we can choose a pure quaternion \( x \) of norm prime to \( p \), such that \( xv \) is pure \((\text{mod } p) \).

We assume as we may that \( p \mid v_1 \), and must choose \( x \) to satisfy

\[
(2) \quad x_1v_1 + x_2v_2 + x_3v_3 \equiv 0, \quad x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \mod p.
\]

Solving \((2)\) in the form \( x_1 = ex_2 + fx_3 \), we reduce \((2)\) to

\[
(1 + e^2)x_2^2 + 2efx_2x_3 + (1 + f^2)x_3^2 \not\equiv 0 \mod p.
\]

---

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

\[
  v = i_1 - i_2v_2 - i_3v_3, \quad 1 + v_2^2 + v_3^2 = pq, \quad q \text{ an integer.}
\]

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

\[
  vd = 0, \quad Nt = p^2?
\]

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

\[
  t_0 = v_3t_2 - v_2t_3, \quad t_1 = v_2t_2 + v_3t_3 \quad \text{(mod } p).\]

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

\[
  t_0 = px_0 + v_3x_1 + v_2x_2, \quad t_1 = px_1 + v_2x_2 + v_3x_3, \quad t_2 = x_2, \quad t_3 = x_3,
\]

where the \( x_i \) are integers, and, on dividing through by \( p \), obtain

\[
  p(x_0^2 + x_1^2) + 2v_3(x_0x_1 + x_2x_3) - 2v_2(x_0x_2 + x_1x_3) + q(x_2^2 + x_3^2) = 1.
\]

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 \( (x_0, \ldots, x_3) \). 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 momentarily], 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, \( p \mid t_0^2 + t_2^2 \) for some \( \alpha \). No two of the following \( p^{2k} \) quaternions are congruent (mod \( p^k \)):

\[
  (e + fi_0)t, \quad e, f = 0, 1, \ldots, p^k - 1.
\]

From \((r + si_0)t = 0\) (mod \( p^k \)) follows \( r = s = 0 \), for

\[
  rt_0 - st_1 = 0, \quad rt_0 + st_1 = 0, \quad r(t_0^2 + t_2^2) = 0 = s(t_0^2 + t_2^2).
\]

**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 \( p | t_0 + t_1^2 \) for \( \alpha = 1, 2, \) and 3; for then \( p | \sum (t_\alpha + t_\alpha^2) = 2t_0 + Nt, \) \( p | t; \) \( (i = 0, 1, 2, 3). \) Let \( \kappa \) denote the number of solutions \( x \) of \( xt = 0, \) and \( \rho \) the number of residues \( ut \) (mod \( p^k \)). The number of solutions \( x \) of \( xt = wt, \) for a given \( w, \) is the same as that of \( (x - w)t = 0, \) hence equals \( \kappa; \) that is, every residue \( ut \) is represented for \( \kappa \) residues \( u, \) whence \( \kappa \rho = p^k. \) By Lemma 5, \( \rho \geq p^2k; \) since \( x = (e + f_i)l \) obviously satisfies \( xt = 0, \) \( \kappa \geq p^2k. \) Hence \( \kappa = \rho = p^2k. \)

**Corollary 2.** If \( p^k \) \( | \) \( Nt \) 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, \( m \) \( | \) \( Nt. \) Then all left-multiples \( ut \) (mod \( m \)) which are pure (mod \( m \)) form an unique set \( \mathcal{M}; \) that is, all pure left-multiples of \( t \) are proportional (mod \( m \)).

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

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

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

**Corollary 4.** Let \( x \) and \( y \) be proper (mod \( m \)), \( Nx = Ny = 0. \) 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 \( m \)), \( m \) \( | \) \( Nv, \) and let \( vw \) be pure (mod \( m \)). Then there exists an integer \( \lambda \) such that \( vw = \lambda v. \)

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 \( k \) \( | \) \( m. \) If \( k \) \( | \) \( z, \) \( k \) \( | \) \( uz. \) If \( k \) \( | \) \( uz, \) \( k \) \( | \) \( \bar{u}uz, \) \( k \) \( | \) \( z. \)

**Lemma 7.** If \( t^\prime, t^\prime\prime, \ldots, t^{(f)} \) are quaternions of odd prime norm \( p, \) then \( t = t^\prime t^\prime\prime \cdots t^{(f)} \) is proper if and only if

\[
\begin{align*}
(t^{(g)})^{(s+1)} & \text{ is proper for } \quad g = 1, 2, \ldots, f - 1.
\end{align*}
\]
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 \( x = ut^{(f+1)} \). If \( x \) is not proper, \( x = \gamma p \), \( \gamma \) integral; and since \( p = i^{(f+1)}t^{(f+1)} \), \( t = y\theta i^{(f+1)} \). Hence \( t^{(f)} = \theta i^{(f+1)} \), since both are right divisors of \( t \) of norm \( p \), \( \theta \) denoting a unit \( \pm 1 \) or \( \pm i \). Thus \( t^{(f)}t^{(f+1)} = \theta p \).

By a similar argument we obtain

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

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

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

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

For if \( x = ut, y = vt, \) and \( Nt = m \), then \( x\bar{y} = uv\bar{u}\bar{v} = muv = 0 \). Conversely, if \( x\bar{y} = 0 \), we apply Lemma 9 and Corollary 4.

**Theorem 6.** Let \( x \) and \( y \) be proper \( \pmod m \), \( m \mid Nx \) 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

\[
m \mid (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3).
\]

**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

\[
\frac{1}{2}(x\bar{y} + \bar{x}y) = \frac{1}{2}(t'at''\bar{b}' + t'bt''\bar{a}') = \frac{1}{2}Nt''[t'(a\bar{b} + b\bar{a})\bar{a}''] = \frac{1}{2}Nt''(a\bar{b} + b\bar{a})Nt' = m_1m_2 \sum a_i\bar{a}_i,
\]

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

**Sufficiency.** From \( x\bar{y} + \bar{x}y = 0 \) and \( \bar{x}x = 0 \) follow
Let $p^r$ be any prime-power dividing $m$. Then \( p^r \mid xy \). Let $p$ be the highest power of $p$ for which $p^r \mid xy$. By Theorem 5, $x$ and $y$ have the same right divisor of norm $p^r$. If $s \geq r$ this result suffices as regards $p$. If $r > s$, we can set $x = ut$, $y = vt$, $Nt = p^s$, whence $uv$ is proper and $p^{r-s} \mid Nv$. Then $p^{r-s} \mid uv$. Hence by Theorem 5, $uv$ 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 $xy = 0 (\bmod p^r)$ is as follows:

\[
\begin{align*}
(11) & \quad x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 = 0 (\bmod p^r), \\
& \quad \begin{cases} (x_0y_1 - x_1y_0) + (x_2y_3 - x_3y_2) = 0 (\bmod p^r), \\
(2) & \quad \begin{cases} (x_0y_3 - x_3y_0) + (x_2y_1 - x_1y_2) = 0 (\bmod p^r). \\
\end{cases}
\end{cases}
\end{align*}
\]

**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), where $\alpha = 1, 2, 3$ is such that $p^r \mid y_\alpha^2 + y_\alpha^2$. Similarly for left divisors with the +’s in (12) changed to −’s.

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

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

\[
\begin{align*}
( - y_0y_2 + y_1y_3)(11) - (y_0y_2 + y_1y_3)(12) + (y_0^2 + y_1^2)(12) = 0, \\
- (y_0y_2 + y_1y_3)(11) + (y_0y_2 - y_1y_3)(12) + (y_0^2 + y_1^2)(12) = 0.
\end{align*}
\]

Hence (11)–(12) 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 $xy = 0$. Incidentally, this gives an alternative proof of Theorem 5.

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

**Corollary 7**. If $x$ is pure, and $v$ is pure and proper (mod $m$), $m \mid Nv$ and $m \mid \sum x_i v_\alpha$, 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

\[
\begin{align*}
x_0v_1 + x_2v_2 - x_3v_3 &= 0, \quad x_0v_3 + x_2v_1 - x_1v_2 = 0, \quad x_0v_1 + x_3v_2 - x_2v_1 = 0 (p^r),
\end{align*}
\]

in which $p \mid v_\alpha$, for each prime-power dividing $m$.
Corollary 8. If \( y \) is proper \((\text{mod } m)\), 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 \( x = ky \) \((\text{mod } m)\) for some integer \( k \).

For then \( x_0y_0 - x_0y_0 \equiv 0 \pmod{p^r}, f, g = 0, 1, 2, 3 \).

The value of \( k \) may sometimes be obtained from the identity
\[
tat = 2(a_0t_0 - \sum a_\alpha t_\alpha)t - aNt.
\]

Corollary 9. If \( m \mid Nx, Ny, \) and \( \sum x_iy_i \), and \( x \) and \( y \) are proper \((\text{mod } m)\), then there is a factorization \( m = m_1m_2 \) such that
\[
(x_0y_1 - x_1y_0) = \pm (x_2y_2 - x_2y_2), \quad (x_0y_2 - x_2y_0) = \pm (x_3y_1 - x_1y_3),
\]
\[
(x_0y_3 - x_3y_0) = \pm (x_2y_2 - x_2y_2),
\]
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 \( \sum x_iy_i \), then \( x \) and \( y \) are proportional \((\text{mod } m)\).

The most interesting special case of Theorem 6 is

Theorem 7. Let \( x \) and \( y \) be proper \((\text{mod } p)\), \( p \) 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
\[
(x_0y_1 + x_1y_0 + x_2y_2 + x_3y_3) = 0 \pmod{p}.
\]

An independent proof involves interesting lemmas:

Lemma 10. If \( Nt = p \), \( p \) cannot divide two of \( \ell_\alpha + \ell_\alpha^2 \) \((\alpha = 1, 2, 3)\).

For if \( p \mid \ell_\alpha + \ell_\alpha^2 \leq p \), then \( \ell_\alpha + \ell_\alpha^2 = p \).

Lemma 11. If \( Nt = p = Nt' \), then exactly \( p \) of the \( p^2 \) left-multiples of \( t \), \((\text{mod } p)\), are also right-multiples of \( t' \).

For by Lemma 10 we can assume \( p \mid \ell_\alpha + \ell_\alpha^2 \) and \( p \mid \ell_\alpha^2 + \ell_\alpha^3 \). By Theorem 5', \( t' \) and \((e+fj)t \) (cf. Lemma 5) have the same left divisors of norm \( p \) if and only if, to modulus \( p \),
\[
e(t_0 + t_1' + t_2' + t_3') + f(t_0' - t_0 + t_1' - t_2' - t_3') = 0,
\]
\[
e(t_0' - t_0 + t_1' - t_2' + t_3') + f(- t_0' - t_1' + t_2' + t_3') = 0.
\]
The determinant is easily seen to be zero \((\text{mod } p)\) while not all the coefficients are zero. Hence there are \( p \) solutions \( e, f \).

Lemma 12. For a given \( y \) such that \( p \mid y \) but \( p \nmid Ny \), there are precisely \( 2p^2 - p \) solutions \( x_0, x_1, x_2, x_3 \) of
(14) \[ y_0x_0 + y_1x_1 + y_2x_2 + y_3x_3 = 0, \quad x_0^2 + x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{p}. \]

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 \( b_t \pm i_2t_a \pm i_2t_b \pm i_2t_c \) in a set \( \mathbb{F} \), 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 \( Q \) of \( \mathbb{F} \). We can easily verify

**Lemma 13.** The twenty-four notationally distinct elements in a set \( \mathbb{F} \), with fixed \( t_0 \), can be expressed by

\[ \eta \mathbf{h}, \]

(15) \[ \eta = 1, \ i_\alpha, (1 + i_\omega)/2^{1/2}, (1 - i_\omega)/2^{1/2}, \ (i_\alpha - i_{\alpha+1})/2^{1/2}, (i_\alpha + i_{\alpha+1})/2^{1/2}, \]

\[ \frac{1}{2}(1 + i_1 + i_2 + i_3) = \nu, i_\omega \nu, \nu, i_\omega \nu, \]

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

Consider the relation between divisors of elements \( x \) and \( x' \) in the same set \( \mathbb{F} \). 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 \( \eta x\mathbf{h} \), as in (15). From \( x = ut \) follows

(16) \[ \eta x\mathbf{h} = \eta \nu \mathbf{h} \cdot \eta \mathbf{h}. \]

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 \( x \).

Trivially, \( x = ut \) implies \( x' = ita \). But the right divisors of \( x \) and \( x' \) are not related in any obvious way. Some light on this question is exhibited by

**Theorem 8.** Let \( x \) be proper \( \pmod{m} \), \( m \mid Nx \). Then \( x \) and \( x' \) have their right divisors of norm \( m \) in the same set \( \mathbb{F} \) if and only if

(17) \[ m \] divides one of \( x_f, x_f \pm x_o \) \( (f \neq g) \), \( x_0 \pm x_1 \pm x_2 \pm x_3 \).

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

(18) \[ 2s_0 = x\theta + \overline{\theta}x, \quad s_0 \] the scalar part of \( x\theta \).

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

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

From (18) we obtain

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

If $x = vt'$, then $2e^2s_0 = \eta t'$, $m = Nt' \mid 2e^2s_0i'$, hence $m \mid s_0$. Conversely, if $m \mid s_0$, $t' = \eta i\bar{i}$ is a right divisor of $20s_0$, hence by (20) of $e^2x$, hence of $x$ ($e^2$ being prime to $m$).

**Theorem 9.** Let $t$ be proper, $Nt = m$. Let $M_1$ and $M_2$ denote, respectively, the set of pure left- and right-multiples of $t$ (mod $m$). Then $M_1$ and $M_2$ can be obtained from each other by interchanges or sign-changes of $i_1$, $i_2$, $i_3$, if and only if

$$\text{two of } i_1, i_2, i_3, i_0, 0 \text{ are equal.}$$

**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 $\pm v' = \eta v\bar{i}$, while $-v' = v' = bi$. Since $v'$ is pure, (17) holds trivially with $v = x$, so that $i$ and $\eta i\bar{i}$ are in the same $E$, whence (21).

**Sufficiency.** If (21) holds, $i$ and $t$ are in the same $E$. By (16), the left-multiples of $t$ are obtained from those of $i$ by permuting and changing signs of $i_1$, $i_2$, $i_3$. The pure left-multiples of $i$ 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 $8f + 7$,

$$r'(n) = 12h(-n), \text{ if } n \equiv 1 \text{ or } 2 (\text{mod } 4),$$
$$= 8h(-n), \text{ if } n \equiv 3 (\text{mod } 8).$$

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

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

$$x, -i_1x_i = i_1x_1 - i_2x_2 - i_3x_3, -i_2x_i = -i_2x_1 - i_3x_2,$$

obtained by changing signs of two $x_i$; four, that is, except for $N[x] = 1$, when only two of them are distinct. With $\phi$ 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 $Q$ (Corollary 1). Define $y = (tx\bar{i})/k = tu - x_0$. If $t$ is replaced by a left-associate $i_d$, $y$ is replaced
by \(-i_3 y_3\), in \([y]\). If \(t\) is changed to \(-t\), \(y\) is unaltered. If \(x\) is replaced by \(x' = -i_3 y_3\), \(x_0 + x' = -i_3 y_3\), and we again obtain \(y\).

Further, \(y\) is proper. For if \(p\|y\), then \(p\|n = Ny\); and \(p\|k\), since \(kx = iy\) and \(x\) is proper. Since \(x_0^2 + n = kl\), \(p\|x_0\). Hence \(p\|tu = y + x_0\). Since \(t\) is proper, \(p\|tu, p\|Nu = l\), contradicting the primitivity of \([k, 2x_0, l]\).

Reciprocally, since \(y = -y\), \(-x_0 + y = -ul\), whence \(iyt = kx\), 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 \(\phi\):

\[
[k, 2(x_0 + h), \cdots, [l, -2x, k].
\]

For, if \(x_0 + x = ut\), then \(x_0 + h + x = (u + h t) t\); and \(-x_0 + x = -ul, (uxu)/l = y = tu - x_0\), since \(y = -y\).

**Corollary 11.** Any two equivalent forms \(\phi\) 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

\[
[b = [k, 2x_0, h], \psi = [h, 2x_0, kl]\].
\]

By assumption,

\[
x_0 + x = ut, \quad Nt = k, \quad (txt)/k = y = tu - x_0, \quad x_0 + y = vt', \quad Nt' = h, \quad (t'yt')/l = z = t'v - x_0.
\]

Hence \(tu = vt'\); since \(Nu = hl\), \(u = vt'\),

\[
x_0 + x = w(t' t), \quad N(t't) = hk, \quad (t'txu)/(hk) = z.
\]

By \(\mathfrak{F} = \mathfrak{F}(y)\) 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 \((vyv)/Nv\) is in \(\mathfrak{F}(y)\).

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

**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 \(\mathfrak{F}(y)\),

\[
txt' = my'.
\]

For, \(x^2 = y^2, (x + y)x = y(x + y), (x + y)x(x + y) = yN(x + y)\). If \(y = -x\), the theorem is trivial: \(y' = x, t = 1\). Hence we can suppose \(x + y \neq 0, x + y = ut, Nv\) a power of 2, \(Nt\) odd; \(txt = m(vyv/Nv)\).

If a proper \([x]\) can be carried into \([y]\) by the process associated with a
primitive class $C$, then $txi = (Nt)y$ 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 $txi = my$, 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, $tx = x_0t$ (mod $m$) for some integer $x_0$. Hence

$$(x_0 + x)i = x_0j - x = x_0j - x_0i = 0,$$ 

$$(x_0 + x)i = mu, \ x_0 + x = ut.$$

**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 $txi = mx$, $Nt = m$, follows $tx = xt$, or

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

Since $x$ is proper, $t_a = g x_{\alpha}$ for some integer $g$, ($\alpha = 1, 2, 3$). The condition $Nt = m$ becomes $t_1 + ng^2 = m$. 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

$$txi = (Nt)x'$$

exists if and only if: (a) $x' = x$, (2), (b) $r$ is even if $Nx = 3$ (8).

On expanding $txi$ we find $txi = (Nt)x$ (mod 2), whence (a) is necessary. To prove the necessity of (b) we have to prove the impossibility of $txi = -mx$ with $Nt$ odd, that is, of $tx = -xt$, $Nt$ odd, $x_1, x_2, x_3$ odd. Expanded, these imply

$$x_3t_1 + x_2t_2 + x_1t_3 = 0, \ x_1t_0 = x_2t_0 = x_3t_0 = 0,$$

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

(γ) $x' = -x$, $Nx \equiv 1$ or 2 (mod 4); (δ) $x' = i_1x_1 + i_2x_2 + i_3x_3$, $x_1 \equiv x_2$ (2).

For (γ), $(x_2i_2 - x_3i_3)x(x_3i_2 - x_2i_3) = (x_2^2 + x_3^2)(-x)$ 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 $n = 2$ (mod 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 occur in (γ). By (a) and (b) we have

**Corollary 12.** If $N = 1$ or 2 (mod 4), $x$ can be transformed into precisely one-third of the vectors in $S(x)$. If $N = 3$ (mod 8), $x$ can be transformed into precisely half the vectors in $S(x)$.
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 $ixt$, where $Nt = p$ and $Nx = n$. Here $t$ and $x$ are unique except that they may be replaced by $\theta t$ and $\theta x\bar{o}$, where $\theta = \pm 1$ or $\pm i\alpha$. If $y$ is changed to $-iyi\bar{s}$, 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 $Q$. Here $p | Nv$, whence $v$ has the same left divisors of norm $p$ as $y = -y = i\bar{v}$. Hence $v = i\bar{x}$, and so on. That $x$ is proper follows from $y = ixt$, $y$ proper.

However, a given proper $[x]$ of norm $n$ gives rise to $p - (-n | p)$ proper sets $[y]$ of norm $p^2n$, since there are $p^2 + 1$ sets $Q$ of norm $p$ and $1 + (-n | p)$ of them make $ixt = 0$ (mod $p$). The latter values $t$ (by Lemma 18) are the left divisors of $x_0 + x$, where $x^2_0 + n = 0$ (mod $p$). If $t$ and $t'$ are not in the same $Q$, $ixt$ and $i'xt'$ are not in the same $[y]$, by the uniqueness feature of Lemma 21. Hence we have

\[ r'(p^2n) = \{p - (-n | p)\}r'(n). \]

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

\[ r''(p^2n) = \{p - (-n | p)\}r''(n), \]

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

\[ r(p^2n) = r(n) + r''(p^2n) = r(n) + \{p - (-n | p)\}r''(n) \]
\[ = r(n) + \{p - (-n | p)\} \{r(n) - r(n/p^2)\}, \]

that is,

\[ r(p^2n) = [p + 1 - (-n | p)]r(n) - [p - (-n | p)]r(n/p^2), \]

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

\[ r(m^2h) = r(h) \cdot \prod \psi(p_i, \alpha_i; h), \]
\[ \psi(p, \alpha; h) = \frac{p^{a+1} - 1}{p - 1} - (-h | p) \frac{p^a - 1}{p - 1}. \]

Also, $r'(m^2h) = r'(h) \cdot \prod \phi(p_i, \alpha_i; h)$, where $\phi(p, \alpha; h) = p^a - (-h | p)p^{a-1}$.
8. Let $h$ have no square factor greater than 1, $m$ odd and positive. We shall prove that the general solution of

$$hm^2 = y_1^2 + y_2^2 + y_3^2$$

in integers $y_a$ such that, if $p \mid y = iy_1 + iy_2 + iy_3$, then

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

is given by $y = tx\bar{t}$, where

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

If $y = tx\bar{t}$, $Ny = Nx(Nt)^2$, whence if (32) holds, $y$ satisfies (30). To see that $y$ also satisfies (31), set $y = ptz = tx\bar{t}$. Then $p^2 \mid Ny = m^2h$, $p \mid m = pm'$. Hence $txm = p^st$, $txm' = st = \lambda (\text{mod } m)$ for some integer $\lambda$ by Corollary 8, $m' \mid \lambda = x_0m'$ since $t$ is proper, $tx = tx_0 (\text{mod } p^2)$, $p^4 \mid (x_0 - x)(x_0 + x)$, $p^4 \mid x_0^2 + h$; $(-h \mid p) = 1$, 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 $tx\bar{t}$. To do this we write $m = pm'$, $r > 0$, $p \mid m'$, and show that $y = t'z', t'$ proper of norm $p^2$, $z$ 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 $y = t'z'$ and contradicts (31). Eliminating in turn each prime-power in $m$ we finally obtain $y = tx\bar{t}$, 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, $p^2 \mid Nu$, $u$ proper (mod $p$). Then $u = tv\bar{t}$, $t$ proper, $Nt = p^r$, $Nv = (Nu)/p^{2r}$.

Case $p \mid y$, $p \mid h$. By (31), $p^2 \mid y$. Set $y = pu$, $m = pm_0$, $Nu = km_0^2$. Since $u$ is proper (mod $p$) and $p^{2r-1} \mid Nu$, $u = tv\bar{t}$, $t$ proper, $Nt = p^{r-1}$, $Nv = km'^2$. Since $p \mid Nu$, $v = tv_0$, $Nt' = p$, and hence $pv = t'v_0\bar{t}'$, where $v' = wt'$. Hence $y = pu = (tt')v_0(\bar{t}t')$. Here $tt'$ must be proper, since $tv$ (a factor of $u$) is proper (mod $p$).

Case $p \mid y$, $(-h \mid p) = 1$. Set $y = p^su$, $u$ proper (mod $p$), $m = pm_0$, $Nu = km_0^2$. Then $u = tv\bar{t}$, $Nt = p^{r-1}$, $Nv = km'^2$. There are two solutions $\pm v_0$ of $v_0^2 = -hm'^2$ (mod $p^2$). Since $p \mid v_0$, the left divisors of norm $p$ of $v_0 + v$ and $-v_0 + v$ cannot be the same. Hence we can set $v_0 + v = t'w$, $Nt' = p^r$, $t'$ proper, and choose the sign of $v_0$ to make $tt'$ proper (Lemma 7). Then $v' = wt' - v_0 = (t't\bar{t}')/p^r$, and $p^r = t'v_0\bar{t}'$, $y = (tt')v_0(\bar{t}t')$.

Case $p \mid y$. 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 \(n \equiv 1 \pmod{4}, x_2 = x_3\) (2);
(c) \([2, 0, n/2]\) carries \(x\) into \((x_1, x_3, -x_2)\) if \(n \equiv 2 \pmod{4}, x_2 = x_3\) (2);
(d) \([4, 2, (n+1)/4]\) carries \(x\) into \((x_2, x_3, x_1)\) or \((x_3, x_1, x_2)\) if \(n \equiv 3 \pmod{8}\), 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