Bull. Korean Math. Soc.
Vol. 12, No. 1, 1975

ON THE FOUR SQUARE THEOREM

BY JUNGHWAN OH AND JEAYOUNG HAN

Introduction.

In this paper we shall consider a particular subring, Hurwitz ring, of real quaternions which, in all ways except for its lack of the commutativity, will look like a Euclidean ring. We show that any element in Hurwitz ring has an associate with non-integral coordinates, and for any prime integer p, there is an element r in Hurwitz ring such that the norm of r is equal to p. We also show that any prime number p can be expressed as a sum of squares of four integers.

Consequently we will prove that every positive integer can be expressed as a sum of squares of four integers.

1. The norm and adjoint of real quaternions.

DEFINITION 1.1. Let Q be ring of real quaternions.

For $a=a_0+a_1i+a_2j+a_3k$ is Q, the adjoint of a, denoted by a^*, is defined by $a^*=a_0-a_1i-a_2j-a_3k$.

DEFINITION 1.2. The norm of a in Q, denoted by $N(a)$, is defined by $N(a)=aa^*$.

Note that for any real number a, $N(a)=a^2$, and if $x\neq 0$, then $x^{-1}=x^*/N(x)$.

The following Lemma which is essential to the present paper will be briefly stated without proof.

LEMMA. (*a*) *The adjoint in Q satisfies*

$$(xy)^*=y^*x^*, \text{ for all } x, y \text{ in } Q.$$

(*b*) *For all x, y in Q*

$$N(xy)=N(x)N(y).$$

2. Integral quaternions.

Now we shall introduce the Hurwitz ring of integral quaternions.

DEFINITION 2.1. Let $\rho=\frac{1}{2}(1+i+j+k)$ and $H=\{m_0\rho+m_1i+m_2j+m_3k;\ m_0, m_1, m_2, m_3$ are in $Z\}$. The set H is called Hurwitz ring of integral quaternions.

The following Lemma is obvious.

LEMMA 2.1. *(a) x^* is in H, for all x in H,*

(b) $N(x)$ is a positive integer, for all nonzero x in H,

DEFINITION 2.2. An element a in H is called a unity if a^{-1} is in H.

LEMMA 2.2. *The element a in H is a unity if and only if the norm of a is 1.*

Proof. Suppose a^{-1} is in H. Then $N(a)$ and $N(a^{-1})$ are positive integers, and $N(a)N(a^{-1})=1$, by Lemma 2.1. Hence $N(a)=1$.

Conversely, if a is in H and $N(a)=1$, then $N(a)=aa^*=1$, and $a^{-1}=a^*$ in H.

DEFINITION 2.3. The element ae or ea is called an associate of a if e is a unity in H.

THEOREM 1. *If a is in H and $N(a)$ is an odd integer, then at least one of its associates has non-integral coordinates.*

Proof. Suppose $N(a)$ is an odd, and $a\in H$ has integral coordinates, then we have $a=(b_0+b_1i+b_2j+b_3k)+(c_0+c_1i+c_2j+c_3k)=s+r$ so that b's are all even integers and each of c_0, c_1, c_2, c_3 has value 0 or 1. Then there are only two cases: one of c's is equal to 1 and the others are all zero or three of them have value 1 and the other is equal to zero.

In the case $r=1+i+j$, we have $r=(1+i+j+k)-k$ and $re=2-ke$, where $e=\frac{1}{2}(1-i-j-k)$. Then the associate of a, $ae=se+2-ke$, has non-integral coordinates. Similarly, the other cases can be shown.

LEMMA 2.3. *If α is in H and m is a positive integer, then there is x in H such that $N(\alpha-xm)<N(m)$.*

Proof. Suppose that $\alpha=t_0\rho+t_1i+t_2j+t_3k$

and
$$x=x_0\rho+x_1i+x_2j+x_3k,$$
where x's are integers yet to be determined,

then

$$\alpha - mx = \frac{1}{2}t_0(1+i+j+k) + t_1 i + t_2 j + t_3 k - \frac{1}{2}mx_0(1+i+j+k)$$
$$- mx_1 i - mx_2 j - mx_3 k$$
$$= \frac{1}{2}(t_0 - mx_0) + \frac{1}{2}(t_0 + 2t_1 - m(x_0 + 2x_1))i$$
$$+ \frac{1}{2}(t_0 + 2t_2 - m(x_0 + 2x_2))j + \frac{1}{2}(t_0 + 2t_3 - m(x_0 + 2x_3))k.$$

We can choose x_0, x_1, x_2, x_3 in succession so that these have absolute values not exceeding $\frac{1}{4}m, \frac{1}{2}m, \frac{1}{2}m, \frac{1}{2}m$; and then $N(\alpha - mx) < N(m)$.

LEMMA 2.4. *If a is in H and $b \neq 0$ in H, then there are c and d such that $a = cb + d$, $N(d) < N(b)$.*

Proof. Let $k = ab^*$ and $m = bb^*$, then there is c in H such that $N(k - mc) < N(m)$. Thus we have $N(ab^* - cbb^*) = N(a - cb)N(b^*) < N(b)N(b^*)$. Since $N(b^*)$ is positive integer, $N(a - cb) < N(b)$. Taking $d = a - cb$, we have $a = cb + d$, where $N(d) < N(b)$.

THEOREM 2. *Every left ideal L of H is a principal left ideal.*

Proof. If $L = (0)$, there is nothing to prove, merely put $u = 0$.

Assume that L has non-zero elements. There is an element $u = 0$ in L whose norm is minimal over the nonzero elements of L. For this u, if y is in L, there is $r = y - xu \in L$ and $N(r) < N(u)$, by Lemma 2.4. Therefore $y - xu = 0$, and $y = xu$. Hence L is the principal left ideal.

DEFINITION 2.4. For a and b in H, and b have a greatest common right divisor $d = (a, b)$ if it satisfies the following conditions;

(a) d is right divisor of a and b,

(b) every right divisor of a and b is right divisor of d.

LEMMA 2.5. *a and b have a greatest right common divisor d, for all a and b in H.*

Proof. Let S be the set of all elements $xa + yb$, where x and y are in H. Then S is a left ideal, and so S is a principal ideal. Since a and b are both in S, d is a common right divisor of a and b, and any such divisor of a and b is also a right divisor of every element of S. Therefore, d is the greatest common right divisor of a and b.

THEOREM 3. *For a in H and $b=m$, a positive integer, there are x and y in H such that $xa+yb=1$ if and only if $(N(a), N(b))=1$.*

Proof. Suppose that there are x and y in H such that $xa+yb=1$.
Then,

$$N(xa)=N(1-by)=(1-my)(1-my^*)=1-my-my^*+m^2N(y),$$

$$N(x)N(a)=1-my-my^*+m^2N(y).$$

Hence $(N(a), N(b))=1$.

Conversely, if there are d_1 and d_2 such that $a=d_1d$ and $b=d_2d$, then $N(d)$ is a common divisor of $N(a)$ and $N(b)$. That is $(N(a), N(b))\geqq N(d)$. Consequently d is a unity. There are x and y in H such that $xa+by=1$.

DEFINITION 2.5. Nonzero element α in H is called a prime in H if $\alpha=ab$ implies that a or b is a unity.

LEMMA 2.6. *Any prime integer p can not be a prime in H.*

Proof. If $p=2$, then $2=(1+i)(1-i)$ is not prime in H.
Suppose p is an odd prime, then there are integers a and b such that

$$0<a, b<p, \ 1+a^2+b^2\equiv 0 \pmod p.$$

Let $s=1-ai-bj$, then $N(s)=1+a^2+b^2\equiv 0 \pmod p$ and $(N(s), p)>1$. By Theorem 3, s and p have a common right divisor d which is not a unity. For s is not a unity, we can have $s=d_1d$ and $p=d_2d$. If d_2 is a unity, d is an associate of p and $s=d_1d_2^{-1}p$. In this case, p divides all the coordinates of a, but it is impossible. Hence $p=d_2d$, where neither d_2 nor d is a unity; that is, p is not a prime.

THEOREM 4. *The norm of r is a prime integer if and only if r is a prime in H.*

Proof. Let $N(r)$ be a prime integer and $r=ab$ for some a and b in H, then $N(a)N(b)=N(r)$ and $N(a)$ or $N(b)$ is 1.
Hence r is a prime in H.

On the other hand, suppose that r in H is a prime and let a prime integer p be a divisor of $N(r)$. By Theorem 3, r and p have a common right divisor

$\bar{r}$ which is not a unity.

Since r is a prime in $H, \bar{r}$ is an associate of r and $N(\bar{r})=N(r)$. Also $p^2=x\bar{r}$ for some x in H and $p=N(x)N(\bar{r})$, so that $N(r)$ is 1 or p. If $N(r)$ were 1, then p would be an associate of r and $\bar{r}$, so that p is prime in H. But it is impossible, by Lemma 2. Hence the norm of r is equal to prime integer p.

3. The four-square theorem.

We now have determined enough of the structures of of H. We shall introduce the classical theorems of Lagrange and Euler to use them effectively to study properties of the integers.

LEMMA 3.1. *If* $2a=m_0^2+m_1^2+m_2^2+m_3^2$, *where* m_0, m_1, m_2, m_3 *are integers, then* $a=n_0^2+n_1^2+n_2^2+n_3^2$, *for some integer* n_0, n_1, n_2, n_3.

LEMMA 3.2. *The product of two integers each a sum of four integral squares is again a sum of four integral squares..*

THEOREM 5. *If p is an odd prime integer, then $4p$ can be expressed as a sum of four integral squares. Furthermore p can be expressed as a sum of four integral squares.*

Proof. Since p is an odd prime integer, we have $p=ab$, for some a and b in H, and $N(a)=N(b)=p$, by Theorem 4. We can also select an associate a' of a whose coordinates are halves of odd integers, by Theorem 1.

$$p=N(a)=N(a')=\left(b_0+\frac{1}{2}\right)^2+\left(b_1+\frac{1}{2}\right)^2+\left(b_2+\frac{1}{2}\right)^2+\left(b_3+\frac{1}{2}\right)^2.$$

References

[1] Ralph. Archibald: *An introduction to theory of numbers.* 1970.

[2] G. E. Andrews: *Number theory.* 1971.

[3] I. N. Herstein: *Topics in algebra.* 1964.

[4] William Judson Leveque: *Topics in number theory.* 1956.

[5] G. H. Hardy and E. M. Whight: *An introduction to the theory of numbers.* 1959.

[6] Nathan Jacobson: *Lectures in abstract algebra.* 1965.

Yonsei University