Journal of Pure and Applied Algebra 217 (2013) 779–785

Contents lists available at SciVerse ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Common left- and right-hand divisors of a quaternion integer[☆]

Mohammed Abouzaid[a], Jarod Alper[b], Steve DiMauro[c], Justin Grosslight[d], Derek Smith[e,*]

[a] MIT, Math Department, Cambridge, MA 02139, United States
[b] Columbia University, Math Department, New York, NY 10027, United States
[c] Silver Spring, MD, United States
[d] Harvard University, History of Science Department, Harvard, MA 02138, United States
[e] Lafayette College, Math Department, Easton, PA 18042, United States

ARTICLE INFO

Article history:
Received 11 October 2007
Received in revised form 13 June 2012
Available online 8 October 2012
Communicated by R. Parimala

MSC: 11-XX; 11A51; 11R52

ABSTRACT

Given a quaternion integer α whose norm is divisible by a natural number m, does there exist a quaternion integer β of norm m dividing α on both the left and right? This problem is a case of the "metacommutation problem", which asks generally for relationships between the many different factorizations of a given integral quaternion. In this paper, we give necessary and sufficient conditions on primitive α of odd norm to ensure the existence of common left- and right-hand divisors, and we characterize the non-trivial sets of such divisors.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

In [1], Cayley solves the quaternion equation

$$Qq' = qQ,$$

where q and q' are given quaternions over $\mathbb{R}$. Here, we address a similar problem, but in the subring H of Hurwitz's integral quaternions, whose definition and important properties are defined in Section 1.1 below. Let α be a primitive quaternion in H whose norm is divisible by the positive integer m. Does α have any common left- and right-hand factors of norm m? That is, do there exist β, γ, and γ' in H such that $[\beta] = m$ and

$$\alpha = \beta\gamma = \gamma'\beta?$$

This problem is a special case of the "metacommutation problem" for H, which asks generally for relationships between the many different factorizations of a given integral quaternion. The theorem at the end of Section 2 provides necessary and sufficient conditions for the existence of common left- and right-hand norm-m factors of α when m is odd. Subsequent theorems in Section 3 characterize the non-trivial sets of common left- and right-hand factors of α.

1.1. Basic properties of H

Hamilton's algebra of quaternions, $\mathbb{H}$, is the 4-dimensional composition algebra over $\mathbb{R}$ for the Euclidean norm. Multiplication in $\mathbb{H}$ is associative but not commutative, and it satisfies the composition law. Following the notation in [2],

☆ Partially supported by NSF grant DMS-9912325 and the EXCEL Scholars program at Lafayette College.
* Corresponding author.
E-mail addresses: abouzaid@math.mit.edu (M. Abouzaid), jarod@math.columbia.edu (J. Alper), sadimauro@gmail.com (S. DiMauro), jgrossl@fas.harvard.edu (J. Grosslight), smithder@lafayette.edu (D. Smith).

0022-4049/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2012.08.003

we denote the inner product of two elements α, β in $\mathbb{H}$ by $[\alpha, \beta]$ and write the norm $[\alpha]$ as an abbreviation for $[\alpha, \alpha]$, so that the composition law is written as

$$[\alpha\beta] = [\alpha][\beta]$$

for all α, β. Other basic properties of $\mathbb{H}$ follow directly from this law (see pages 68–69 of [2] for proofs). Defining an involutionary conjugation map by $\overline{\alpha} = 2[\alpha, 1] - \alpha$, we have for all α, β, γ in $\mathbb{H}$ the "scaling laws"

$$[\alpha\beta, \alpha\gamma] = [\alpha][\beta, \gamma] \qquad [\alpha\beta, \gamma\beta] = [\alpha, \beta][\beta],$$

the "braid laws"

$$[\beta, \overline{\alpha}\gamma] = [\alpha\beta, \gamma] = [\alpha, \gamma\overline{\beta}],$$

and other conjugation laws such as

$$\overline{\alpha\beta} = \overline{\beta}\overline{\alpha} \qquad \overline{\alpha}\alpha = \alpha\overline{\alpha} = [\alpha].$$

For coordinates, every element α in $\mathbb{H}$ can be written as a linear combination of an orthonormal basis $\{1, i, j, k\}$, with multiplication determined by $i^2 = j^2 = k^2 = ijk = -1$.

$\mathbb{H}$ contains two natural subrings of integers,

$$\mathsf{L} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$$

and

$$\mathsf{H} = \left\{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \mathbb{Z} + \frac{1}{2}\right\},$$

that are geometrically similar to the 4-dimensional lattices I_4 and D_4, respectively [3], scaled so that the norms of vectors are integral and the smallest non-zero vectors have norm 1. The ring H was first studied by Hurwitz in [4]; it contains L, studied by Lipschitz. Of the two, only the Hurwitzian ring H is a unique factorization domain, a property required for the main results of Section 3. (The theorem at the end of Section 2 can be adapted to hold in L alone.)

We refer to the group of units in L and H by L^* and H^*, respectively, finding that

$$\mathsf{L}^* = \{\pm 1, \pm i, \pm j, \pm k\}$$

and

$$\mathsf{H}^* = \left\{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\right\},$$

so that $|\mathsf{L}^*| = 8$ and $|\mathsf{H}^*| = 24$. The number of elements in H^* whose inner product with 1 equals

$$1, \frac{1}{2}, 0, -\frac{1}{2}, -1$$

is

$$1, 8, 6, 8, 1,$$

the elements having multiplicative order

$$1, 6, 4, 3, 2.$$

The automorphism group $Aut(\mathsf{H}) = Aut(\mathsf{L})$ is a group of order 24, consisting of all maps determined by $i \to i'$ and $j \to j'$, with i' and j' chosen from $\{\pm i, \pm j, \pm k\}$ such that $[i', 1] = [j', 1] = [i', j'] = 0$. In particular, $Aut(\mathsf{H})$ is transitive on elements that have the same inner product with 1. For example, each of the 8 units $\frac{-1\pm i\pm j\pm k}{2}$ can be taken to $\omega = \frac{-1+i+j+k}{2}$ under $Aut(\mathsf{H})$.

Let $\alpha \in \mathsf{H}$ be primitive, which means that it cannot be expressed as $n\alpha'$ with $\alpha' \in \mathsf{H}$ and $n \in \mathbf{Z}$ with $n > 1$. Define

$$L_m(\alpha) = \{\beta \in \mathsf{H} \mid \alpha = \beta\gamma \text{ with } \gamma \in \mathsf{H} \text{ and } [\beta] = m\}$$

and

$$R_m(\alpha) = \{\beta \in \mathsf{H} \mid \alpha = \gamma\beta \text{ with } \gamma' \in \mathsf{H} \text{ and } [\beta] = m\}$$

as the sets of left- and right-hand factors of α with norm m. Our main problem is determining

$$L_m(\alpha) \cap R_m(\alpha)$$

for a given α and $m|[\alpha]$.

2. Existence of odd-norm two-sided divisors

In this section, we provide necessary and sufficient conditions to ensure that a primitive quaternion integer α of odd norm has a common left and right divisor. We refer to an element of H that is also in L as being of type (I), and otherwise being of type (II). If $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, we set $a_i' = a_i$ if α has type (I), and $a_i' = 2a_i$ if α has type (II); and we define b_i' for $\beta = b_0 + b_1 i + b_2 j + b_3 k$ similarly. For instance,

$$\alpha = \frac{1}{2} + \frac{3}{2}i + \frac{1}{2}j - \frac{5}{2}k$$

is of type (II) with norm $[\alpha] = 9$, $a_1 = 3/2$, and $a_1' = 3$.

Theorem 1. *Suppose $\alpha \in \mathsf{H}$ is primitive, and let m be an odd integer such that $m|[\alpha]$. Then*

$$L_m(\alpha) \cap R_m(\alpha) \neq \emptyset$$

if and only if there exists a $\beta \in \mathsf{H}$ such that $[\beta] = m$ and $a_i' b_j' \equiv a_j' b_i' \pmod m$ for all $i \neq j$.

It is essential that m be odd in this proof. For example, let $\alpha = 2i + j + k$, so that $\alpha = \beta\gamma = \gamma'\beta$ for $\beta = 1 + i$, $\gamma = 1 + i + j$, and $\gamma' = 1 + i + k$. But then $a_0' = b_2' = 0$ and $a_2' = b_0' = 1$, so that $a_0' b_2' \not\equiv a_2' b_0' \pmod 2$. We do not understand the behavior of even-norm divisors.

Proof. If we assume that $L_m(\alpha) \cap R_m(\alpha) \neq \emptyset$, then there exist integral quaternions β, γ, and γ' such that $[\beta] = m$ and $\alpha = \beta\gamma = \gamma'\beta$. Therefore $\gamma' = \beta\gamma\beta^{-1}$ must be integral, and we now compute its coordinates. First, see that

$$[\gamma', 1] = [\beta\gamma\beta^{-1}, 1] = [\beta\gamma, 1\overline{\beta^{-1}}] = \frac{1}{[\beta]}[\beta\gamma, \beta] = \frac{1}{[\beta]}[\beta][\gamma, 1] = [\gamma, 1],$$

which implies that γ and γ' are both of type (I) or both of type (II). Next, we compute

$$[\gamma', i] = [\beta\gamma\beta^{-1}, i] = \frac{1}{[\beta]}[\beta\gamma, i\beta].$$

Since $i\beta = -b_1 + b_0 i - b_3 j + b_2 k$ and $\beta i = -b_1 + b_0 i + b_3 j - b_2 k$, we have $i\beta = \beta i - 2b_3 j + 2b_2 k$. Thus,

$$\begin{aligned}
[\gamma', i] &= \frac{1}{m}[\beta\gamma, \beta i - 2b_3 j + 2b_2 k] \\
&= \frac{1}{m}[\beta\gamma, \beta i] + \frac{1}{m}[\beta\gamma, -2b_3 j + 2b_2 k] \\
&= [\gamma, i] + \frac{1}{m}[\alpha, -2b_3 j + 2b_2 k] \\
&= [\gamma, i] + \frac{1}{m}(-2a_2 b_3 + 2a_3 b_2).
\end{aligned}$$

Since both γ and γ' are of the same type, if γ is to be integral it must follow that

$$\frac{2}{m}(-a_2 b_3 + a_3 b_2) \in \mathbb{Z}.$$

Since $\gcd(2, m) = 1$, one can check that regardless of the types of α and β, $a_2' b_3' \equiv a_3' b_2' \pmod m$. Similar calculations yield

$$[\gamma', j] = [\gamma, j] + \frac{2}{m}(-a_3 b_1 + a_1 b_3)$$

and

$$[\gamma', k] = [\gamma, k] + \frac{2}{m}(-a_1 b_2 + a_2 b_1),$$

which imply $a_1' b_3' \equiv a_3' b_1' \pmod m$ and $a_1' b_2' \equiv a_2' b_1' \pmod m$.

To get the other three conditions of the theorem, we compute

$$2[\gamma', i] = 2[\alpha\beta^{-1}, i] = \frac{2}{[\beta]}[\alpha\overline{\beta}, i] = \frac{2}{m}(-a_0 b_1 + a_1 b_0 - a_2 b_3 + a_3 b_2)$$

$$2[\gamma', j] = 2[\alpha\beta^{-1}, j] = \frac{2}{[\beta]}[\alpha\overline{\beta}, j] = \frac{2}{m}(-a_0 b_2 + a_2 b_0 + a_1 b_3 - a_3 b_1)$$

$$2[\gamma', k] = 2[\alpha\beta^{-1}, k] = \frac{2}{[\beta]}[\alpha\overline{\beta}, k] = \frac{2}{m}(-a_0 b_3 + a_3 b_0 - a_1 b_2 + a_2 b_1).$$

In the final expression of each equation, the numerator of the sum of the final two terms is divisible by m, so the same is true for the sum of the first two terms, leading to the three conditions

$$a_0'b_1' \equiv a_1'b_0' \pmod{m}, \qquad a_0'b_2' \equiv a_2'b_0' \pmod{m}, \quad \text{and} \quad a_0'b_3' \equiv a_3'b_0' \pmod{m}.$$

For the other direction of the theorem, suppose we have $[\beta] = m$ such that $a_i'b_j' \equiv a_j'b_i'(m)$ for all $i \neq j$. We need to show that β divides α on the left and right, which is the same as showing that $\gamma' = \alpha\beta^{-1}$ and $\gamma = \beta^{-1}\alpha$ are integral quaternions.

The previously displayed three expressions for $2[\gamma', i]$, $2[\gamma', j]$, and $2[\gamma', k]$, together with the assumptions $a_i'b_j' \equiv a_j'b_i'(m)$, show that each of $[\gamma', i]$, $[\gamma', j]$, and $[\gamma', k]$ is in $(\frac{1}{4})\mathbb{Z}$, since the four corresponding terms a_ib_j are in $(\frac{1}{4})\mathbb{Z}$. Moreover, if one of the four terms a_ib_j is not in $(\frac{1}{2})\mathbb{Z}$, then none of these evenly-many terms are. Either way, we find that each of $[\gamma', i]$, $[\gamma', j]$, and $[\gamma', k]$ is in fact in $(\frac{1}{2})\mathbb{Z}$. We then only need to see that the equation

$$[\gamma', 1]^2 + [\gamma', i]^2 + [\gamma', j]^2 + [\gamma', k]^2 = [\gamma'] \in \mathbb{Z}$$

implies that $[\gamma', 1] \in (\frac{1}{2})\mathbb{Z}$, with all of $[\gamma', 1]$, $[\gamma', i]$, $[\gamma', j]$, and $[\gamma', k]$ in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$. We conclude that γ' is integral, and a similar calculation shows that γ is integral. □

3. Characterizing the intersection sets

Let $\alpha \in \mathsf{H}$ be primitive and let m be odd. To characterize the different possibilities for

$$L_m(\alpha) \cap R_m(\alpha),$$

we translate the problem into a similar one regarding units.

By unique factorization in H, if $\alpha = \beta\gamma = \gamma'\beta$, then

$$\alpha = \beta u \cdot u^{-1}\gamma = \gamma' v^{-1} \cdot v\beta,$$

for arbitrary units u, v, give all 2-term factorizations of α with one factor having norm $[\beta]$. Thus, if $A_r(\beta)$ and $A_l(\beta)$ are, respectively, the sets of right and left associates of β, then

$$L_m(\alpha) \cap R_m(\alpha) = A_r(\beta) \cap A_l(\beta),$$

an equality that does not necessarily hold if α is not primitive.

For any $\psi \in \mathsf{H}$, define

$$U_l(\psi) = \{u \mid u\psi = \psi v \ \text{ for some } v \in \mathsf{H}^*\}$$

and

$$U_r(\psi) = \{v \mid u\psi = \psi v \ \text{ for some } u \in \mathsf{H}^*\}.$$

Since multiplication by β is an orthogonal transformation up to scaling, we conclude that

$$L_m(\alpha) \cap R_m(\alpha) = A_r(\beta) \cap A_l(\beta) \sim U_l(\beta) \sim U_r(\beta),$$

where $\sim$ denotes geometrical similarity.

As a simple example corresponding to the conditions in Theorem 2, $\alpha = 1 + 5i + 2j + 5k$ has norm $[\alpha] = 55$. If we set $m = 5$, we find that

$$L_5(\alpha) \cap R_5(\alpha) = \{\pm(1 + 2j), \pm(2 - j)\}$$

and

$$U_l(\beta) = U_r(\beta) = \{\pm 1, \pm j\},$$

which are geometrically similar sets of pairs of orthogonal vectors.

Several things can be said about $U_l(\psi)$ (and similarly about $U_r(\psi)$).

Lemma 1. *If $\psi \in \mathsf{H}$, then $U_l(\psi)$ is a subgroup of H^* of order 2, 4, 6, or 24.*

Proof. H^* is finite, and $U_l(\psi)$ is closed since $u\psi = \psi v$ and $u'\psi = \psi v'$ imply $uu'\psi = u\psi v' = \psi v v'$, proving that $U_l(\psi)$ is a subgroup of H^*. Since the order of H^* is 24 and the elements of $U_l(\psi)$ come in $\pm$ pairs, the possible orders for $U_l(\psi)$ are 2, 4, 6, 8, 12, and 24. But H^* does not have a subgroup of order 12. Also, the Lipschitzian units are the unique subgroup of H^* of order 8, so if $1\psi = \psi 1$, $i\psi = \psi u_1$, $j\psi = \psi u_2$, and $k\psi = \psi u_3$, then

$$\frac{1}{2}(1 + i + j + k)\psi = \psi\frac{1}{2}(1 + u_1 + u_2 + u_3),$$

with $\frac{1}{2}(1 + u_1 + u_2 + u_3) \in \mathsf{H}^*$, so order 8 is not a possibility. □

Lemma 4, which characterizes the ψ giving each possible order for $U_l(\psi)$, makes use of the following two lemmas. For conjugation $\epsilon^{-1}\psi\epsilon$, we write ψ^{ϵ}.

Lemma 2. *$U_l(\psi) = U_l(\psi u)$ for any $u \in \mathsf{H}^*$.*

Proof. If $u'\psi = \psi v'$, then $u'\psi u = \psi v' u = \psi u v$ for some $v \in \mathsf{H}^*$; and if $u'\psi u = \psi u v$, then $u'\psi = u'\psi u u^{-1} = \psi u v u^{-1}$. □

Lemma 3. *Let $\psi \in \mathsf{H}$ and $u, \delta \in \mathsf{H}^*$ with $u \neq \pm 1$. Then $u\psi = \psi u^{\delta}$ if and only if ψ is a linear combination of δ and $u\delta$.*

Proof. Consider a basis $\{1, u, \beta_1, \beta_2\}$ of $\mathbb{H}$ such that $[\beta_i, 1] = [\beta_i, u] = 0$. Then $\{\delta, u\delta, \beta_1\delta, \beta_2\delta\}$ is also a basis, so there exist real numbers a, b, c_1, and c_2 such that

$$\psi = a\delta + bu\delta + c_1\beta_1\delta + c_2\beta_2\delta.$$

Thus,

$$u\psi = au\delta + bu^2\delta + u(c_1\beta_1\delta + c_2\beta_2\delta),$$

and

$$\begin{aligned} \psi u^{\delta} &= au\delta + bu^2\delta + c_1\beta_1 u\delta + c_2\beta_2 u\delta \\ &= au\delta + bu^2\delta + bu^2\delta + c_1\overline{u}\beta_1\delta + c_2\overline{u}\beta_2\delta \\ &= au\delta + bu^2\delta + \overline{u}(c_1\beta_1\delta + c_2\beta_2\delta), \end{aligned}$$

the latter calculation using the fact that if $[\beta_i, 1] = [\beta_i, u] = 0$, then $\beta_i u = \overline{u}\beta_i$. These expressions for $u\psi$ and ψu^{δ} are equal if and only if

$$u(c_1\beta_1\delta + c_2\beta_2\delta) = \overline{u}(c_1\beta_1\delta + c_2\beta_2\delta),$$

which is only true for non real u precisely when

$$c_1\beta_1\delta + c_2\beta_2\delta = 0.$$

Since $\{1, u, \beta_1, \beta_2\}$ is a basis, this is equivalent to saying that $\psi = a\delta + bu\delta$. □

We are now in a position to provide necessary and sufficient conditions on the size of $|U_l(\psi)|$. The proof briefly makes use of the cosets of D_4 in D_4^*; for a fuller discussion, see page 62 of [2].

Lemma 4. *Let $\psi \in \mathsf{H}$ have $[\psi]$ odd, and let $u_1, u_2 \in \mathsf{H}^*$ and $a, b \in \mathbb{Z}$. Then*

1. *$|U_l(\psi)| = 4$ if and only if $\psi = au_1 + bu_2$ with $[u_1, u_2] = 0$ and $a \neq 0 \neq b$;*
2. *$|U_l(\psi)| = 6$ if and only if $\psi = au_1 + bu_2$ with $[u_1, u_2] = \frac{1}{2}$ and $a \neq 0 \neq b$;*
3. *$|U_l(\psi)| = 24$ if and only if $\psi = au_1$.*

Proof. Suppose that $u\psi = \psi v$ for $u, v \in \mathsf{H}^*$. Since $[\psi]$ is odd, u and v map to the same coset of D_4 in D_4^*, which implies that $v = u^{\delta}$ for some $\delta \in \mathsf{H}^*$. If $u \neq \pm 1$, then Lemma 3 implies that $\psi = a\delta + bu\delta$ for some $a, b \in \mathbb{R}$ (and in fact $a, b \in \mathbb{Z}$).

With this in mind, we prove the forward implication in each of the three cases. If $|U_l(\psi)| = 4$, then up to $Aut(\mathsf{H})$, $U_l(\psi) = \{\pm 1, \pm i\}$. Since $i \neq \pm 1$ and $i\psi = \psi i^{\delta}$ for some $\delta \in \mathsf{H}^*$, we have

$$\psi = a\delta + bi\delta = au_1 + bu_2$$

with $[u_1, u_2] = [\delta, i\delta] = [1, i][\delta] = 0$. Similarly, if $|U_l(\psi)| = 6$, then up to $Aut(\mathsf{H})$, $U_l(\psi) = \{\pm 1, \pm\omega, \pm\overline{\omega}\}$. Since $\omega \neq \pm 1$ and $\omega\psi = \psi\omega^{\delta}$ for some $\delta \in \mathsf{H}^*$, we have

$$\psi = a\delta + b\omega\delta = au_1 + bu_2$$

with $[u_1, u_2] = \frac{1}{2}$. Finally, if $|U_l(\psi)| = 24$, then $U_l(\psi) = \mathsf{H}^*$, and so

$$\psi = a\delta + bi\delta = a'\delta' + b'j\delta'$$

for some $\delta, \delta' \in \mathsf{H}^*$ and $a, b, a', b' \in \mathbb{Z}$. But this implies

$$(a + bi)\delta = (a' + b'j)\delta'$$

and so

$$\frac{1}{a^2 + b^2}(a - bi)(a' + b'j) = \delta(\delta')^{-1} \in \mathsf{H}^*,$$

which in view of $aa' - ba'i + ab'j - bb'k = (a - bi)(a' + b'j)$ is only possible for odd $[\psi]$ if one of a, b and one of a', b' are equal to 0.

For the reverse implications, we proceed as follows. If $\psi = au_1 + bu_2$ with $[u_1, u_2] = 0$, then $\psi u_1^{-1} = a + bu_2u_1^{-1}$ with $[u_2u_1^{-1}, 1] = 0$. By Lemma 2, $|U_l(\psi)| = |U_l(\psi u_1^{-1})|$, and up to $Aut(\mathsf{H})$ we may assume that $u_2u_1^{-1} = i$, so we may assume that $\psi = a + bi$. Obviously, $\pm 1, \pm i \in U_l(\psi)$, and if $U_l(\psi)$ contains any other units then $U_l(\psi) = \mathsf{H}^*$ by Lemma 1. But it can be checked that, for example, $j(a + bi) \neq (a + bi)u$ for any $u \in \mathsf{H}^*$, using the facts that $a \neq 0 \neq b$ and $[\psi]$ is odd.

Similarly, if $\psi = au_1 + bu_2$ with $[u_1, u_2] = \frac{1}{2}$, then $\psi u_1^{-1} = a + bu_2u_1^{-1}$ with $[u_2u_1^{-1}, 1] = \frac{1}{2}$. Up to $Aut(\mathsf{H})$ we may assume that $u_2u_1^{-1} = -\omega$, and so $\psi = a + b(-\omega)$. Obviously, $\pm 1, \pm\omega, \pm\overline{\omega} \in U_l(\psi)$, and if $U_l(\psi)$ contains any other units then $U_l(\psi) = \mathsf{H}^*$ by Lemma 1. But it can be checked that, for example, $i(a + b(-\omega)) \neq (a + b(-\omega))u$ for any $u \in \mathsf{H}^*$.

Finally, if $\psi = au_1$, then $U_l(\psi) = \mathsf{H}^*$ since ψ is just an integer multiple of an element of H^*. □

Our final lemma shows that $|L_m(\psi) \cap R_m(\psi)|$ is invariant up to associates.

Lemma 5. *For any $u \in \mathsf{H}^*$,*

$$|L_m(\psi) \cap R_m(\psi)| = |L_m(u\psi) \cap R_m(u\psi)| = |L_m(\psi u) \cap R_m(\psi u)|.$$

Proof. If $\beta \in L_m(\psi) \cap R_m(\psi)$, then there exist integral quaternions γ, γ' such that $\psi = \beta\gamma = \gamma'\beta$. Multiplying on the left by u, we see that $u\psi = u\beta\gamma = u\gamma'u^{-1}u\beta$ which clearly implies that $u\beta \in L_m(u\psi) \cap R_m(u\psi)$, and so $|L_m(\psi) \cap R_m(\psi)| \leq |L_m(u\psi) \cap R_m(u\psi)|$. Repeat this argument by multiplying $u\psi$ on the left by u^{-1} to see that $|L_m(u\psi) \cap R_m(u\psi)| \leq |L_m(\psi) \cap R_m(\psi)|$. A similar argument establishes the result for right associates. □

We now prove the two theorems that characterize the sizes of intersection sets. Recall the definition of a_i' given at the beginning of Section 2.

Theorem 2. *Let $\alpha \in \mathsf{H}$ be primitive and let m be an odd integer. Then $|L_m(\alpha) \cap R_m(\alpha)| = 4$ if and only if*

$$\alpha = a_0 + a_1i + a_2j + a_3k,$$

up to multiplication by units and $Aut(\mathsf{H})$, with $a_2' \equiv a_3' \equiv 0 \pmod m$ and the existence of integers a, b relatively prime to m such that $a^2 + b^2 = m$ and $a_0'b \equiv a_1'a \pmod m$.

Proof. If $|L_m(\alpha) \cap R_m(\alpha)| = 4$, then there exist integral quaternions β, γ, and γ' with $\alpha = \beta\gamma = \gamma'\beta$ with $[\beta] = m$. From the discussion at the beginning of this section,

$$L_m(\alpha) \cap R_m(\alpha) \sim U_l(\beta),$$

so by Lemma 4, $\beta = au_1 + bu_2$ for integers a, b and integral quaternion units u_1, u_2 such that $[\beta] = a^2 + b^2 = m$ and $[u_1, u_2] = 0$.

By Lemma 2 (using $u = u_1^{-1}$), we may assume that $u_1 = 1$, and then by $Aut(\mathsf{H})$ that $u_2 = i$, so $\beta = a + bi$. Theorem 1 then implies the congruences

$$\begin{aligned} a_0'b &\equiv a_1'a \pmod m \\ a_0'0 &\equiv a_2'a \pmod m \\ a_0'0 &\equiv a_3'a \pmod m. \end{aligned}$$

To conclude that $a_2 \equiv a_3 \equiv 0$, it is enough to know that $(a, m) = 1$. But if $(a, m) = d > 1$, then $a^2 + b^2 = m$ implies that $(b, m) = d$, so that $d|\beta$, which contradicts the primitivity of α.

For the other direction, let $\beta = a + bi$ with the given conditions on a and b. The six congruences of Theorem 1 are then satisfied, so $\alpha = \beta\gamma = \gamma'\beta$ for integral quaternions γ, γ'. By Lemma 4,

$$|L_m(\alpha) \cap R_m(\alpha)| = |U_l(\beta)| = 4. \quad \square$$

Theorem 3. *Let α be a primitive integral quaternion and m an odd integer. Then $|L_m(\alpha) \cap R_m(\alpha)| = 6$ if and only if*

$$\alpha = a_0 + a_1i + a_2j + a_3k,$$

up to multiplication by units and $Aut(\mathsf{H})$, with $a_1' \equiv a_2' \equiv a_3' \pmod m$ and the existence of integers a, b relatively prime to m such that $a^2 + ab + b^2 = m$ and $a_0'b \equiv a_1'(2a + b) \pmod m$.

Proof. If $|L_m(\alpha) \cap R_m(\alpha)| = 6$, then there exist integral quaternions β, γ, and γ' with $\alpha = \beta\gamma = \gamma'\beta$ and $[\beta] = m$. From the discussion at the beginning of this section,

$$L_m(\alpha) \cap R_m(\alpha) \sim U_l(\beta),$$

so by Lemma 4, $\beta = au_1 + bu_2$ for integers a, b and integral quaternion units u_1, u_2 such that $[\beta] = a^2 + ab + b^2 = m$ and $[u_1, u_2] = \frac{1}{2}$.

By Lemma 2 (using $u = u_1^{-1}$), we may assume that $u_1 = 1$, and then by $Aut(\mathsf{H})$ that $u_2 = -\omega$, so

$$\beta = a + b(-\omega) = \frac{1}{2}((2a + b) - bi - bj - bk).$$

Theorem 1 then implies the congruences

$$a'_0 b \equiv a'_1(2a+b) \pmod{m}$$
$$a'_1 b \equiv a'_2 b \pmod{m}$$
$$a'_1 b \equiv a'_3 b \pmod{m}.$$

If $(a, m) = d > 1$, then $a^2 + ab + b^2 = m$ implies that $(b, m) = d$, so that $d|\beta$ and thus $d|\alpha$, contradicting the primitivity of α. So we may assume that $(a, m) = (b, m) = 1$, which implies that the last three congruences above are equivalent to $a'_1 \equiv a'_2 \equiv a'_3(m)$.

For the other direction, let $\beta = a + b(-\omega) = \frac{1}{2}((2a+b) - bi - bj - bk)$ with the given conditions on a and b. The six congruences of Theorem 1 are then satisfied, so $\alpha = \beta\gamma = \gamma'\beta$ for integral quaternions γ, γ'. By Lemma 4,

$$|L_m(\alpha) \cap R_m(\alpha)| = |U_l(\beta)| = 6. \quad \square$$

Acknowledgment

We thank an anonymous referee for many helpful comments and suggestions.

References

[1] A. Cayley, On the quaternion equation $qQ - Qq' = 0$, Mess. Math. 14 (1885) 108–112. Also in the Collected Mathematical Papers of Arthur Cayley, Cambridge University Press, 1897, pp. 300–304.
[2] J. Conway, D. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, AK Peters, Ltd., 2003.
[3] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices, and Groups, second ed., Springer-Verlag, 1993.
[4] A. Hurwitz, Über die Zahlentheorie der Quaternionen, Nachr. Ges. der Wiss. zu Göttingen (1896) 314–340.