CONNECTIONS BETWEEN THE ARITHMETIC AND THE GEOMETRY OF LIPSCHITZ INTEGERS

ANTÓNIO MACHIAVELO AND LUÍS ROÇADAS

Abstract. Some relationships between the arithmetic and the geometry of Lipschitz and Hurwitz integers are here presented. In particular, it is shown that the vector product of two left multiples of a Lipschitz integer α with any other Lipschitz integer is still a left multiple of α, and that the vector product of a Lipschitz integer α with two other such integers orthogonal to it is both a left and a right multiple of α. Some possible connections with factorization algorithms are mentioned.

1. Introduction

Frénicle de Bessy seems to have been the first to notice that from two different decompositions of an integer n as a sum of two squares one can obtain a factorization of n ([D], vol. I, cap. XIV, p. 360). This amounts to the fact that a decomposition $n = a^2+b^2$ gives a factorization $n = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$, and if one has another decomposition $n = c^2 + d^2$, then, using the Euclidean algorithm in $\mathbb{Z}[i]$, one can find the gcd of $a + bi$ and $c + di$, whose norm yields a factor of n.

As Bachet de Méziriac conjectured and Lagrange proved, every number is a sum of four squares ([D], vol. II, cap. VIII, p. 275). Such a decomposition of an integer n yields a factorization $n = \alpha\bar{\alpha}$ in the ring of Hurwitz integers. Since this ring is both a left and a right Euclidean domain, it is natural to wonder if two distinct decompositions of a number as a sum of four squares could yield, in a manner analogous to the above, a factorization of that number. Moreover, while there is no known fast algorithm to decompose a number as a sum of two squares, there is a very efficient probabilistic algorithm, due to Rabin and Shallit [RS], to express a number as a sum of four squares. Therefore, if all worked well, one would get in this manner an interesting factorization algorithm.

However, if one has two decompositions $n = \alpha\bar{\alpha} = \beta\bar{\beta}$, it is not always the case that α and β will have a non-trivial gcd. In fact, for a number

Date: 11/06/2011.

2010 *Mathematics Subject Classification.* Primary 11R52; Secondary 11A51.

Key words and phrases. Hurwitz integers, Lipschitz integers, factorization, orthogonality.

that is a product of two odd primes, $n = pq$, only a small (for p and q big) fraction, exactly $\frac{p+q+2}{(p+1)(q+1)}$, of all possible pairs α, β will have a gcd whose norm is neither 1 nor n. But, in [P], Gordon Pall proves a series of interesting results (namely, theorems 6 and 7), which imply, in particular, that given two quaternions α and β with integral pairwise coprime coordinates, if they are orthogonal and have the same norm, then they either have the same right divisors, or the same left divisors, or both. This suggests looking for orthogonal decompositions of an integer as a sum of four squares, i.e. orthogonal integral quaternions whose norm is that integer.

It was this line of thought that made us study ways of constructing quaternions that are orthogonal to a given quaternion, namely using the vector product, and that led to the discovery of the main results here presented, namely theorems 4.3 and 4.4.

2. Quaternions, Lipschitz and Hurwitz integers

We start by recalling that the quaternion ring $\mathbb{H}$ is the division ring formed by the additive group $\mathbb{R}^4$ endowed with the only multiplication determined (so one gets a ring structure) by choosing $\mathbf{e}_1$ as the multiplicative unit and by the relations:

$$\mathbf{e}_2^2 = \mathbf{e}_3^2 = \mathbf{e}_4^2 = \mathbf{e}_2\mathbf{e}_3\mathbf{e}_4 = -1,$$

where $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ is the canonical basis of $\mathbb{R}^4$. Usually, in this context, one denotes the elements of this basis by $1, i, j, k$, respectively. Given a quaternion $u = a+bi+cj+dk$, its *conjugate* is defined by $\bar{u} = a-bi-cj-dk$, and its *norm* is $\mathrm{N}(u) = u\bar{u}$.

The quaternions with integral coordinates are called *Lipschitz integers*, and they form a subring of $\mathbb{H}$ that we will denote by $\mathcal{L}$. This is almost a left Euclidean ring for the norm, in the sense that for any $\alpha, \beta \in \mathcal{L}$ one can find $q, r \in \mathcal{L}$ such that $\alpha = \beta q + r$ and $\mathrm{N}(r) \leq \mathrm{N}(\beta)$, but a strict inequality cannot always be guaranteed (and the same for right division). In fact one needs only to slightly enlarge $\mathcal{L}$ by adding the quaternions whose coordinates are all halves of odd numbers to obtain a (left and right) Euclidean ring. This yields the set $\mathcal{H} = \mathcal{L} \cup (\omega + \mathcal{L})$, with $\omega = \frac{1}{2}(1+i+j+k)$, whose elements are called *Hurwitz integers*. One can easily show that any Hurwitz integer has both a left and a right associate which is a Lipschitz integer.

In particular, every left or right ideal of $\mathcal{H}$ is principal, and from this, a sort of unique factorization into primes can be deduced for *primitive* Hurwitzian integers, i.e. those not divisible by a rational prime. We recall that a *Hurwitz prime* is simply an Hurwitz integer whose norm is a rational prime.

Theorem 2.1 (Unique Factorization Theorem). *To each factorization of the norm n of a primitive Hurwitzian integer α into a product $p_1p_2\cdots p_{k-1}p_k$ of rational primes, there is a factorization*

$$\alpha = \pi_1\pi_2\cdots\pi_{k-1}\pi_k$$

of α into a product of Hurwitzian primes modelled on *that factorization of n, that is, with $\mathrm{N}(\pi_i) = p_i$.*

Moreover, if $\alpha = \pi_1\pi_2\cdots\pi_{k-1}\pi_k$ is any one factorization modelled on $p_1p_2\cdots p_{k-1}p_k$, then all the others have the form

$$\alpha = \pi_1\varepsilon_1\cdot\varepsilon_1^{-1}\pi_2\varepsilon_2\cdot\varepsilon_2^{-1}\pi_2\varepsilon_3\cdot\ \cdots\ \cdot\varepsilon_{k-1}^{-1}\pi_{k-1}\varepsilon_k\cdot\varepsilon_k^{-1}\pi_k,$$

where $\varepsilon_1,\ldots,\varepsilon_k \in \mathcal{H}^*$, i.e. the factorization on a given model is unique up to unit-migration.

This result is essentially contained in [L] (p. 434), where Lipschitz proves that integral quaternions have that same sort of unique factorization up to factors of norm 2. For a modern proof see Theorem 2, p. 57 in [CS].

Given $m \in \mathbb{N}$, a quaternion $\alpha = a + bi + cj + dk \in \mathcal{L}$ is said to be *primitive modulo m* if $(a, b, c, d, m) = 1$. In [P] (theorem 1), Pall proves the following result:

Theorem 2.2. *If $\alpha \in \mathcal{L}$ is primitive modulo m, where m is odd and positive with $m \mid \mathrm{N}(\alpha)$, then α has exactly a set of eight right divisors of norm m, in $\mathcal{L}$, all of them left-associated. One has an analogous result for left divisors.*

Notice that while theorem 2.1 relates factorizations modelled on the same prime decomposition of the norm, theorem 2.2 gives information about factorizations of a primitive quaternion modelled on different prime decomposition of its norm. For example, if $\alpha = \pi_1\pi_2\pi_3$ is a factorization of a primitive quaternion α corresponding to $\mathrm{N}(\alpha) = p_1p_2p_3$, and $\alpha = \pi_2'\pi_1'\pi_3'$ is a factorization corresponding to $\mathrm{N}(\alpha) = p_2p_1p_3$, then it follows from the last theorem that $\pi_1\pi_2$ and $\pi_2'\pi_1'$ are right associates, and therefore π_3 and π_3' are left associates.

3. Orthogonality and Arithmetic

From the expression for the product of two quaternions, u and v, one readily sees that, for the inner product $u \cdot v$,

$$u \cdot v = \frac{1}{2}\left(u\bar{v} + v\bar{u}\right). \tag{3.1}$$

This very simple observation can be used to obtain some curious relations between common divisors, the inner product and orthogonality, as it will be demonstrated in this section. In what follows, we will use the notation $u \perp v$ to mean that the quaternions u and v are orthogonal, i.e. $u \cdot v = 0$.

Theorem 3.1. *For any $u, v, w \in \mathbb{H}$, one has*

$$(uv) \cdot (uw) = \mathrm{N}(u)\,(v \cdot w).$$

In particular, if $\alpha, \beta \in \mathcal{L}$ have a common left divisor τ, then $\mathrm{N}(\tau) \mid \alpha \cdot \beta$. One has analogous results for right common divisors.

Proof. All follows immediately from:

$$2\,(uv) \cdot (uw) = uv\bar{w}\bar{u} + uw\bar{v}\bar{u} = u\,(v\bar{w} + w\bar{v})\,\bar{u} = 2\,(v \cdot w)\ \mathrm{N}(u).$$

□

Corollary 3.2. *Let $\epsilon, \delta \in \{1, i, j, k\}$ with $\epsilon \neq \delta$. Then, for any $\alpha \in \mathbb{H}$, $\alpha\epsilon \perp \alpha\delta$ and $\epsilon\alpha \perp \delta\alpha$.*

Proof. This is an immediate consequence of the previous proposition, and the fact that $\epsilon \perp \delta$. □

It follows from theorem 6 in [P] that two non-associate Hurwitzian primes cannot be orthogonal. We show here that this can be directly deduced from the unique factorization theorem.

Theorem 3.3. *If $\alpha, \beta \in \mathcal{H}$ are primes with the same norm, and $\alpha \perp \beta$, then each one is a left and right associate of the other.*

Proof. Let $p = \mathrm{N}(\alpha) = \mathrm{N}(\beta)$. From $\alpha \perp \beta$ one gets that $\alpha\bar{\beta} = -\beta\bar{\alpha}$. Now, if the quaternion $\gamma = \alpha\bar{\beta}$ is not primitive, then $m \mid \gamma$ for some $m \in \mathbb{N}$ with $m > 1$. But then, from $m^2 \mid \mathrm{N}(\gamma) = p^2$, it follows that $m = p$. But then $\alpha\bar{\beta} = p\varepsilon = \varepsilon p$, for some unit ε. Since $p = \beta\bar{\beta}$, one gets $\alpha = \varepsilon\beta$. From $\beta\bar{\alpha} = -\alpha\bar{\beta} = p\varepsilon$, one gets $\beta = -\varepsilon\alpha$ (and in this case one sees that $\varepsilon^2 = -1$, and therefore $\varepsilon = \pm i, \pm j, \pm k$).

If γ is primitive, then $\alpha\bar{\beta}$ and $-\beta\bar{\alpha}$ are two factorizations of γ modelled on $\mathrm{N}(\gamma) = pp$, and the unique factorization theorem implies that α and β are right associates.

Finally note that $\alpha \perp \beta \Rightarrow \bar{\alpha} \perp \bar{\beta}$, which allows to deduce the left version of the result from its right version, and vice-versa. □

With non-primes one can obtain examples that are a little more interesting. For instance, from the previous corollary, it follows that if π and ρ are any two quaternions, then $\pi i \rho$ and $\pi\rho$ have the same norm and are orthogonal. The question of what exactly is the left greatest common divisor of these two quaternions, led to:

Theorem 3.4. *Let $\gamma = z + wj \in \mathcal{L}$, with $z, w \in \mathbb{Z}[i]$, be an odd quaternion (i.e. γ has an odd norm). Then:*

$$(i\gamma, \gamma)_R = 1 \qquad \Longleftrightarrow \qquad (z, w) = 1 \quad (\textit{in } \mathbb{Z}[i])$$

Proof. It is clear that if $\delta \mid z$ and $\delta \mid w$, with $\delta \in \mathbb{Z}[i]$, then δ is a left divisor of $i\gamma$, since of course $\delta \mid \gamma$ and it commutes with i. Therefore, $(z, w) = (\delta) \Rightarrow (i\gamma, \gamma)_R \subseteq (\delta)_R$.

On the other hand, putting $I = (i\gamma, \gamma)_R$, and since $i\gamma = zi + wk$, $\gamma i = zi - wk$, one has:

$$2zi = i\gamma + \gamma i \in I$$

and

$$2wk = i\gamma - \gamma i \in I.$$

Hence:

$$2z, 2w \in I.$$

Now, $(2, \mathrm{N}(\gamma)) = 1$ implies that there are $x, y \in \mathbb{Z}$ such that $2x + \gamma\bar{\gamma}y = 1$. In particular, there is $x \in \mathbb{Z}$ with $2x \equiv 1 \pmod{I}$. From this one concludes that $z, w \in I$, and so, if these are coprime, it follows that $I = 1$. □

Note that from an algorithm to compute $\pi i \rho$ from the quaternion $\pi\rho$ one gets a factorization algorithm for integers. To exemplify this, suppose we have a semi-prime number $n = pq$ with p and q to be determined. Using an algorithm like the one in [RS], one can find $\alpha \in \mathcal{L}$ such that $\mathrm{N}(\alpha) = n$, and one has $\alpha = \pi\rho$, for some primes $\pi, \rho \in \mathcal{H}$. If one could somehow determine $\pi i \rho$, then using the Euclidean algorithm, one would get π, and therefore p and q.

4. The vector product in $\mathbb{H}$ and the arithmetic of $\mathcal{L}$

We start by recalling the notion of vector product in $\mathbb{R}^n$.

Definition 4.1. For $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n-1} \in \mathbb{R}^n$, define their vector product by

$$\times(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n-1}) = \mathbf{u}_1 \times \mathbf{u}_2 \times \cdots \times \mathbf{u}_{n-1} := \begin{vmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ \vdots & \vdots & \cdots & \vdots \\ u_{n-1,1} & u_{n-1,2} & \cdots & u_{n-1,n} \\ \mathbf{e}_1 & \mathbf{e}_2 & \cdots & \mathbf{e}_n \end{vmatrix}$$

(with the obvious meaning), where $\mathbf{e}_i$ is the i-th vector of the canonical basis of $\mathbb{R}^n$, and $u_{i,j}$ is the j-th coordinate of the vector $\mathbf{u}_i$, on that same basis.

It easily follows from this definition that, for any vectors $\mathbf{u}_i, \mathbf{v}_j, \mathbf{v} \in \mathbb{R}^n$, where $i, j = 1, \ldots, n-1$, one has:

(1) $(\mathbf{u}_1 \times \mathbf{u}_2 \times \cdots \times \mathbf{u}_{n-1}) \cdot \mathbf{v} = \begin{vmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ \vdots & \vdots & \cdots & \vdots \\ u_{n-1,1} & u_{n-1,2} & \cdots & u_{n-1,n} \\ v_1 & v_2 & \cdots & v_n \end{vmatrix}$

(2) $(\mathbf{u}_1 \times \mathbf{u}_2 \times \cdots \times \mathbf{u}_{n-1}) \perp \mathbf{u}_i$, for all $i = 1, \ldots, n-1$.

(3) $(\mathbf{u}_1 \times \mathbf{u}_2 \times \cdots \times \mathbf{u}_{n-1}) \cdot (\mathbf{v}_1 \times \mathbf{v}_2 \times \cdots \times \mathbf{v}_{n-1}) = \det(\mathbf{u}_i \cdot \mathbf{v}_j)$.

From this last relation, one sees that, for any $\alpha, \beta, \gamma \in \mathbb{H}$,

$$\mathrm{N}(\alpha \times \beta \times \gamma) = (\alpha \times \beta \times \gamma) \cdot (\alpha \times \beta \times \gamma) = \begin{vmatrix} \mathrm{N}(\alpha) & \alpha \cdot \beta & \alpha \cdot \gamma \\ \alpha \cdot \beta & \mathrm{N}(\beta) & \beta \cdot \gamma \\ \alpha \cdot \gamma & \beta \cdot \gamma & \mathrm{N}(\gamma) \end{vmatrix},$$

from which one easily gets

$$\mathrm{N}(\alpha \times \beta \times \gamma) = \mathrm{N}(\alpha\beta\gamma) - \mathrm{N}(\alpha)(\beta \cdot \gamma)^2 - \mathrm{N}(\beta)(\alpha \cdot \gamma)^2 - \\ - \mathrm{N}(\gamma)(\alpha \cdot \beta)^2 + 2(\alpha \cdot \beta)(\alpha \cdot \gamma)(\beta \cdot \gamma).$$

In particular, if $\beta \perp \alpha$ and $\gamma \perp \alpha$, then $\mathrm{N}(\alpha) \mid \mathrm{N}(\alpha \times \beta \times \gamma)$. It follows from theorem 2.2 that $\alpha \times \beta \times \gamma$ has a left and a right divisor both with the same norm as α. We will show that, in both cases, α is that divisor. In order to do that, we need the following result.

Lemma 4.2. *Let $\alpha = a + bi + cj + dk \in \mathcal{L}$ be a primitive quaternion, and let $g_1 = (a, b)$, $g_2 = (c, d)$, and $x_0, y_0, z_0, t_0 \in \mathbb{Z}$ be such that: $ax_0 + by_0 = g_1$, $cz_0 + dt_0 = g_2$. Then the $\mathbb{Z}$-module $\alpha^\perp \cap \mathcal{L}$ is generated by the quaternions:*

$$g_2(x_0 + y_0 i) - g_1(z_0 + t_0 i)j, \quad \frac{1}{g_1}(b - ai), \quad \frac{1}{g_2}(d - ci)j$$

Proof. Suppose we are given $\alpha = a+bi+cj+dk \in \mathcal{L}$, primitive. We want to find all vectors in $\mathcal{L} \cap \alpha^\perp$. Put $g_1 = (a, b)$, $g_2 = (c, d)$, and let $x_0, y_0, z_0, t_0 \in \mathbb{Z}$ be such that:

$$ax_0 + by_0 = g_1 \tag{4.1}$$

$$cz_0 + dt_0 = g_2 \tag{4.2}$$

Now, the elements $\gamma = x + yi + zj + tk \in \mathcal{L}$ such that

$$ax + by + cz + dt = 0. \tag{4.3}$$

must satisfy

$$\begin{aligned} ax + by &= r_1 g_1 \\ cz + dt &= r_2 g_2, \end{aligned}$$

for some $r_1, r_2 \in \mathbb{Z}$ with $r_1 g_1 + r_2 g_2 = 0$. Because α is primitive, $(g_1, g_2) = 1$, and therefore there exists $r \in \mathbb{Z}$ such that $r_1 = r g_2$ and $r_2 = -r g_1$. It then follows from the well known caracterization of the solutions of linear Diophantine equations that:

$$\begin{aligned} x &= r_1x_0 + \frac{b}{g_1}s = rg_2x_0 + \frac{b}{g_1}s \\ y &= r_1y_0 - \frac{a}{g_1}s = rg_2y_0 - \frac{a}{g_1}s \\ z &= r_2z_0 + \frac{d}{g_2}u = -rg_1z_0 + \frac{d}{g_2}u \\ t &= r_2t_0 - \frac{c}{g_2}u = -rg_1t_0 - \frac{c}{g_2}u, \end{aligned} \tag{4.4}$$

for some $s, u \in \mathbb{Z}$. □

Theorem 4.3. *Given $\alpha \in \mathcal{L}$, and $\beta, \gamma \in \mathcal{L}$ such that $\beta \perp \alpha$ and $\gamma \perp \alpha$, one has*

$$\alpha \times \beta \times \gamma \in \alpha\mathcal{L} \cap \mathcal{L}\alpha.$$

Proof. Let $\alpha = a+bi+cj+dk \in \mathcal{L}$, which may be assumed to be a primitive, without loss of generality. Let $g_1 = (a, b)$, $g_2 = (c, d)$, and $x_0, y_0, z_0, t_0 \in \mathbb{Z}$ be as in theorem 4.2. Since, by that result, the $\mathbb{Z}$-module $\alpha^\perp \cap \mathcal{L}$ is generated by the quaternions: $\beta_1 = g_2(x_0 + y_0i) - g_1(z_0 + t_0i)j, \beta_2 = \frac{1}{g_1}(b - ai), \beta_3 = \frac{1}{g_2}(d - ci)j$, it is enough to check the validity of the claimed statement for the products $\alpha \times \beta_1 \times \beta_2$, $\alpha \times \beta_1 \times \beta_3$, and $\alpha \times \beta_2 \times \beta_3$. Now, more or less straighforward computations show that:

$$\begin{aligned} \alpha \times \beta_2 \times \beta_3 &= \alpha(-j)\frac{1}{g_1g_2}(a + bi)(c - di) \\ &= \frac{1}{g_1g_2}(a + bi)(c + di)(-j)\alpha. \\ \alpha \times \beta_1 \times \beta_2 &= \alpha(g_2i - j(b - ai)(z_0 - t_0i)) \\ &= (-g_2i + j(b + ai)(z_0 - t_0i))\alpha. \\ \alpha \times \beta_1 \times \beta_3 &= \alpha(g_1i + k(d + ci)(y_0 - x_0i)) \\ &= (g_1i + k(d + ci)(y_0 + x_0i))\alpha. \end{aligned}$$

□

Using corollary 3.2, one sees that, for example, $\alpha \times \alpha i \times \alpha j \in \alpha\mathcal{L} \cap \mathcal{L}\alpha$. While doing some computational experimentation, we noticed that, for example, $\alpha \times \alpha i \times \beta \in \alpha\mathcal{L}$. This led to the discovery of the next result. In its proof, one needs to compute several vector products, for which it was found convenient to consider the exterior algebra, over $\mathbb{R}$:

$$\bigwedge \mathbb{H} = \bigwedge^0 \mathbb{H} \oplus \bigwedge^1 \mathbb{H} \oplus \bigwedge^2 \mathbb{H} \oplus \bigwedge^3 \mathbb{H} \oplus \bigwedge^4 \mathbb{H}$$

where

$$\bigwedge^0 \mathbb{H} \simeq \bigwedge^4 \mathbb{H} \simeq \mathbb{R}$$

$$\bigwedge^1 \mathbb{H} \simeq \bigwedge^3 \mathbb{H} \simeq \mathbb{H}.$$

One also makes free use of the unique $\mathbb{R}$-linear application $\bigwedge^3 \mathbb{H} \to \mathbb{H}$ such that, for $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} \subset \{1, i, j, k\}$ satisfying $\varepsilon_r \neq \pm\varepsilon_s$, for all $r, s \in \{1, 2, 3\}$ with $r \neq s$,

$$\varepsilon_1 \wedge \varepsilon_2 \wedge \varepsilon_3 \mapsto \varepsilon_1\varepsilon_2\varepsilon_3$$

which is a (linear) isomorphism and the image of $\alpha \wedge \beta \wedge \gamma$ is precisely $\alpha \times \beta \times \gamma$.

Theorem 4.4. *Given $\alpha, \beta, \gamma, \delta \in \mathcal{L}$, one has*

$$\alpha\beta \times \alpha\gamma \times \delta \in \alpha\mathcal{L}.$$

Proof. By (multi)linearity, it is enough to show that the claimed result holds for $\beta, \gamma, \delta \in \{1, i, j, k\}$. Let then $\alpha = a + bi + cj + dk$, with $a, b, c, d \in \mathbb{Z}$, and $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{1, i, j, k\}$. One has:

$$\alpha\varepsilon_1 \wedge \alpha\varepsilon_2 = (a\varepsilon_1 + bi\varepsilon_1 + cj\varepsilon_1 + dk\varepsilon_1) \wedge (a\varepsilon_2 + bi\varepsilon_2 + cj\varepsilon_2 + dk\varepsilon_2) =$$

$$\begin{array}{rcrcrcrc} = a^2\,(\varepsilon_1 \wedge \varepsilon_2) & + & ab\,(\varepsilon_1 \wedge i\varepsilon_2) & + & ac\,(\varepsilon_1 \wedge j\varepsilon_2) & + & ad\,(\varepsilon_1 \wedge k\varepsilon_2) & + \\ ab\,(i\varepsilon_1 \wedge \varepsilon_2) & + & b^2\,(i\varepsilon_1 \wedge i\varepsilon_2) & + & bc\,(i\varepsilon_1 \wedge j\varepsilon_2) & + & bd\,(i\varepsilon_1 \wedge k\varepsilon_2) & + \\ ac\,(j\varepsilon_1 \wedge \varepsilon_2) & + & bc\,(j\varepsilon_1 \wedge i\varepsilon_2) & + & c^2\,(j\varepsilon_1 \wedge j\varepsilon_2) & + & cd\,(j\varepsilon_1 \wedge k\varepsilon_2) & + \\ ad\,(k\varepsilon_1 \wedge \varepsilon_2) & + & bd\,(k\varepsilon_1 \wedge i\varepsilon_2) & + & cd\,(k\varepsilon_1 \wedge j\varepsilon_2) & + & d^2(k\varepsilon_1 \wedge k\varepsilon_2). & \end{array}$$

For ε_2 one now has only three non-trivial cases to consider, up to sign, depending on whether $\varepsilon_2\,\varepsilon_1^{-1} = i, j, k$:

(i) $\varepsilon_2 = i\varepsilon_1$:

$$\begin{aligned} \alpha\varepsilon_1 \wedge \alpha i\varepsilon_1 \wedge \varepsilon_3 &= (a^2 + b^2)\,\varepsilon_1 \wedge i\varepsilon_1 \wedge \varepsilon_3 - (c^2 + d^2)\,j\varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3 + \\ &\quad (ac - bd)\,(k\varepsilon_1 \wedge \varepsilon_1 \wedge \varepsilon_3 + j\varepsilon_1 \wedge i\varepsilon_1 \wedge \varepsilon_3) + \\ &\quad (ad + bc)\,(k\varepsilon_1 \wedge i\varepsilon_1 \wedge \varepsilon_3 + \varepsilon_1 \wedge j\varepsilon_1 \wedge \varepsilon_3). \end{aligned}$$

Now, one has to consider four cases for ε_3, up to sign: $\varepsilon_3/\varepsilon_1 = 1, i, j, k$. For $\varepsilon_3 = \varepsilon_1$, one gets, identifying $\varepsilon_i \wedge \varepsilon_j \wedge \varepsilon_k$ with $\varepsilon_i\varepsilon_j\varepsilon_k$,

$$\begin{aligned} \alpha\varepsilon_1 \times \alpha i\varepsilon_1 \times \varepsilon_1 &= \big(-(c^2 + d^2)i - (ac - bd)k + (ad + bc)j\big)\,\varepsilon_1^3 = \\ &= (-ak + bj - ci + d)c + (aj + bk - c - di)d)\varepsilon_1^3 \\ &= \alpha(-ck + dj)\varepsilon_1^3. \end{aligned}$$

Analogously, one obtains:

$$\begin{aligned}\alpha\varepsilon_1 \times \alpha i\varepsilon_1 \times i\varepsilon_1 &= \alpha(-cj-dk)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha i\varepsilon_1 \times j\varepsilon_1 &= \alpha(ak+bj)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha i\varepsilon_1 \times k\varepsilon_1 &= \alpha(-aj+bk)\varepsilon_1^3\end{aligned}$$

(j) $\varepsilon_2 = j\varepsilon_1$

$$\begin{aligned}\alpha\varepsilon_1 \wedge \alpha j\varepsilon_1 \wedge \varepsilon_3 &= (a^2+c^2)\,\varepsilon_1 \wedge j\varepsilon_2 \wedge \varepsilon_3 + (b^2+d^2)\,i\varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3\\ &\quad +(ab+cd)\,(i\varepsilon_1 \wedge j\varepsilon_1 \wedge \varepsilon_3 + \varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3)\\ &\quad +(ad-bc)\,(k\varepsilon_1 \wedge j\varepsilon_1 \wedge \varepsilon_3 - \varepsilon_1 \wedge i\varepsilon_1 \wedge \varepsilon_3)\end{aligned}$$

Now, according to whether $\varepsilon_3\,\varepsilon_1^{-1} = 1, i, j, k$, one obtains:

$$\begin{aligned}\alpha\varepsilon_1 \times \alpha j\varepsilon_1 \times \varepsilon_1 &= \alpha(bk-di)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha j\varepsilon_1 \times i\varepsilon_1 &= \alpha(-ak+ci)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha j\varepsilon_1 \times j\varepsilon_1 &= \alpha(-bi-dk)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha j\varepsilon_1 \times k\varepsilon_1 &= \alpha(ai+ck)\varepsilon_1^3\end{aligned}$$

(k) $\varepsilon_2 = k\varepsilon_1$

$$\begin{aligned}\alpha\varepsilon_1 \wedge \alpha k\varepsilon_1 \wedge \varepsilon_3 &= (a^2+d^2)\,\varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3 - (b^2+c^2)\,i\varepsilon_1 \wedge j\varepsilon_1 \wedge \varepsilon_3\\ &\quad +(ab-cd)\,(i\varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3 - \varepsilon_1 \wedge j\varepsilon_1 \wedge \varepsilon_3)\\ &\quad +(ac+bd)\,(j\varepsilon_1 \wedge k\varepsilon_1 \wedge \varepsilon_3 + \varepsilon_1 \wedge i\varepsilon_1 \wedge \varepsilon_3)\end{aligned}$$

Again, according to whether $\varepsilon_3\,\varepsilon_1^{-1} = 1, i, j, k$, one obtains:

$$\begin{aligned}\alpha\varepsilon_1 \times \alpha k\varepsilon_1 \times \varepsilon_1 &= \alpha(ci-bj)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha k\varepsilon_1 \times i\varepsilon_1 &= \alpha(aj+di)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha k\varepsilon_1 \times j\varepsilon_1 &= \alpha(-ai+dj)\varepsilon_1^3\\ \alpha\varepsilon_1 \times \alpha k\varepsilon_1 \times k\varepsilon_1 &= \alpha(-bi-cj)\varepsilon_1^3\end{aligned}$$

□

One obviously has a right version of this result. However, it is not true that $\alpha\beta \times \alpha\gamma \times \delta \in \mathcal{L}\alpha$, as can be seen by taking $\alpha = 1+2i, \beta = \delta = 1+i$, and $\gamma = 1+j$.

5. Final remarks

As pointed out in the introduction, the results here presented where obtained while investigating a possible extension, to integral quaternions, of the method of factoring an integer from two of its representations as a sum of two squares. Using results of Pall, this led us to look for integral quaternions that are orthogonal to a given one. To construct these later ones, we turned to the vector product, just to find that this did not yield what we where looking for, but nevertheless yielded results that do not seem at all trivial.

In the end, integral quaternions do encode factoring information about integers, and therefore it is natural to expect that there should exist subexponential factorization methods using quaternions. We hope that others are stimulated by this paper to find these algortihms.

Acknowledgements. This work was supported in part by *Fundação para a Ciência e a Tecnologia*, through the *Centro de Matemática da Universidade do Porto* (`http://www.fc.up.pt/cmup`), and the *Centro de Matemática da Universidade de Trás-os-Montes e Alto Douro* (`http://cmutad.utad.pt`).

References

[CS] John H. Conway, Derek Smith, *On Quaternions and Octonions*, AK Peters 2003.

[D] L. E. Dickson, *History of the Theory of Numbers*, AMS Chelsea Publishing, 1992.

[L] M. Lipschitz, *Recherches sur la transformation, par des substituitions réelles, d'une somme de deux ou de trois carrés en elle-même*, Journal de Mathématiques Pures et Appliqués **2** (1886), 373–439.

[P] Gordon Pall, *On the Arithmetic of Quaternions*, Transactions of the A. M. S. 47 (1940), 487–500.

[RS] Michael O. Rabin and Jeffery O. Shallit, *Randomized Algorithms in Number Theory*, Communications on Pure and Applied Mathematics **XXXIX** (1986), S239–S256.

[S] Pierre Samuel, *Théorie Algébrique des Nombres* (2éme edition), Hermann 1971.

Departamento de Matemática, Faculdade de Ciências da Universidade do Porto, Rua do Campo Alegre, 4169-007 Porto, Portugal
E-mail address: `ajmachia@fc.up.pt`

Departamento de Matemática, Universidade de Trás-os-Montes, Quinta de Prados, 5001-801 Vila Real, Portugal
E-mail address: `rocadas@utad.pt`