SUMS OF SQUARES AND ORTHOGONAL INTEGRAL VECTORS

LEE M. GOSWICK, EMIL W. KISS, GÁBOR MOUSSONG, NÁNDOR SIMÁNYI

Abstract. Two vectors in $\mathbb{Z}^3$ are called *twins* if they are orthogonal and have the same length. The paper describes twin pairs using cubic lattices, and counts the number of twin pairs with a given length. Integers M with the property that each integral vector with length $\sqrt{M}$ has a twin are called twin-complete. They are completely characterized modulo a famous conjecture in number theory. The main tool is the decomposition theory of Hurwitz integral quaternions. Throughout the paper we made a concerted effort to keep the exposition as elementary as possible.

1. Introduction and main results

An *icube* in $\mathbb{Z}^n$ of dimension k is a sequence $(v_1, \dots, v_k)$ of k nonzero vectors in $\mathbb{Z}^n$ that are pairwise orthogonal and have the same length. The subgroup generated by $v_1, \dots, v_k$ is called the corresponding *cubic lattice*. The common *length* of the vectors v_i is denoted by $\|v_i\|$, and is called the *edge length* of the icube. By the *norm* of v_i we shall mean $\mathrm{N}(v_i) = \|v_i\|^2$ (a similar convention is used also for Gaussian integers and quaternions). A *twin pair* is a 2-dimensional icube in $\mathbb{Z}^3$.

In this paper we investigate how icubes can be *constructed, counted,* and *extended.* We shall consider the case $n = 3$. The main results are the following.

- Theorem 5.10 counts all twin pairs with a given edge length.
- Proposition 1.3 and Corollary 5.11 show that a twin pair can be extended to a 3-dimensional icube if and only if its edge length is an integer.
- Theorem 1.5 and Corollary 1.6 investigate the existence and uniqueness of 3-dimensional cubic lattices containing a single integral vector and the extension of single vectors to twins.
- Theorem 1.8 and Corollary 1.10 characterize twin-complete numbers.
- The above results are based on the following representation theorems:
  $k = 1$: Theorem 4.2 and Theorem 4.6;
  $k = 2$: Theorem 5.4;
  $k = 3$: Theorem 3.3 and Corollary 3.9.

1991 *Mathematics Subject Classification.* 11R52, 52C07.

Key words and phrases. Cubic lattice, Euler rotation matrix, Hurwitz integral quaternion.

Second author supported by Hungarian Nat. Sci. Found. (OTKA) Grant No. NK72523, third author supported by Hungarian Nat. Sci. Found. (OTKA) Grant No. T047102, fourth author supported by the National Science Foundation, grants DMS-0457168 and DMS-0800538.

In the rest of the Introduction, we put these results into context.

The problem of *construction* and *counting* for 3-dimensional icubes in $\mathbb{Z}^3$ has been solved by A. Sárközy [Sar61]. To formulate his main result, we use a construction discovered by Euler. The following well-known facts show how to obtain rotations in $\mathbb{R}^3$. Throughout the paper we identify $v = (v_1, v_2, v_3) \in \mathbb{R}^3$ with the pure quaternion $V(v) = v_1 i + v_2 j + v_3 k$.

Theorem 1.1 (see [CS03], Section 3)**.** *Let $\mathbb{H}^* = \mathbb{H} \setminus \{0\}$ denote the set of nonzero quaternions, and V the space of all quaternions with zero real part. For $\alpha \in \mathbb{H}^*$, let $M(\alpha)$ denote the matrix of the transformation $\alpha(\,\cdot\,)\alpha^{-1} : V \to V$ expressed in the standard basis (i, j, k). Then there exists a surjective linear representation $\rho : \mathbb{H}^* \to SO(3, \mathbb{R})$ such that*

(1) $\ker(\rho) = \mathbb{R}^*$.
(2) *The matrix of $\rho(\alpha)$ in the standard basis (i, j, k) is*

$$M(\alpha) = \frac{1}{d} \begin{pmatrix} m^2 + n^2 - p^2 - q^2 & -2mq + 2np & 2mp + 2nq \\ 2mq + 2np & m^2 - n^2 + p^2 - q^2 & -2mn + 2pq \\ -2mp + 2nq & 2mn + 2pq & m^2 - n^2 - p^2 + q^2 \end{pmatrix},$$

where $\alpha = m + ni + pj + qk$ and $d = m^2 + n^2 + p^2 + q^2$. We note that the restriction of the representation ρ to the unit sphere S^3 of $\mathbb{H}$ is the adjoint representation of S^3 with the kernel $\{1, -1\}$, being also the universal covering of the real projective space $SO(3, \mathbb{R})$.

In what follows, we shall concern ourselves with the *Euler matrix* $E(\alpha) = dM(\alpha)$. We are interested in $E(\alpha)$ when its entries are integers. Call such a matrix *primitive* if the greatest common divisor of its nine entries is 1. Similarly, an icube (or a single integral vector) is primitive if the nk entries are relatively prime.

Theorem 1.2 (Sárközy, [Sar61])**.** *If $m, n, p, q \in \mathbb{Z}$, then $E(m+ni+pj+qk)$ is primitive if and only if $\gcd(m, n, p, q) = 1$ and d is odd. Every primitive 3-dimensional icube in $\mathbb{Z}^3$ can be obtained from such an Euler matrix by permuting columns and changing the sign of the third column if necessary.*

This theorem is analyzed in Section 3 and in Corollary 5.12. Sárközy went on to count all 3-dimensional icubes in $\mathbb{Z}^3$ with a given edge length d.

We next look at the question of *extension.* Our first observation puts an obvious limitation on those vectors that can be extended to a 3-dimensional icube in $\mathbb{Z}^3$.

Proposition 1.3. *Let $(v_1, \ldots, v_n)$ be an n-dimensional icube in $\mathbb{Z}^n$. If n is odd, then its edge length is an integer.*

Proof. Let d denote this length. The volume of the cube is d^n, which is an integer, since it is the determinant of the integer matrix $(v_1, \ldots, v_n)$. We have that d^2 is

also an integer, since the vectors have integer components, which implies d^{n-1} is an integer. Therefore, $d = d^n/d^{n-1}$ is rational, and, moreover, an integer. □

This observation makes it easy to answer the following: which 1-dimensional icubes (that is, which vectors in $\mathbb{Z}^3$) can be extended to a 3-dimensional icube? It turns out that the trivial necessary condition given by Proposition 1.3 is sufficient.

Theorem 1.4. *A vector in $\mathbb{Z}^3$ is contained in a 3-dimensional icube if and only if its length is an integer.*

Proof. Let $u = (a, b, c)$ be a primitive integral vector, whose length d is an integer, so $a^2 + b^2 + c^2 = d^2$. We may assume that a is odd. It has been known since at least [Car15] that in this case there exist $m, n, p, q \in \mathbb{Z}$ such that u is exactly the first column of the corresponding Euler matrix. Thus, the columns of this matrix extend u to the desired icube.

If x is a non-primitive vector of integer length, then it can be written uniquely as gu, where $g \in \mathbb{Z}$ and $u \in \mathbb{Z}^3$ is primitive. Then the length of u is also an integer, so it extends to an icube (u, v, w). Therefore, (gu, gv, gw) extends $x = gu$. □

Theorem 4.2 also yields Theorem 1.4, but by using quaternions (see Remark 4.3). When u is primitive, the cubic lattice generated by any 3-dimensional icube containing u is always the same (see Theorem 1.5).

The next question is this: which 2-dimensional icubes in $\mathbb{Z}^3$ can be extended to a 3-dimensional icube? Again, the necessary condition that the length be an integer is sufficient (see Corollary 5.11).

Having surveyed a few results concerning 3-dimensional icubes, we now turn our attention to the 2-dimensional case. From now on by an icube we shall always mean a 3-dimensional icube in $\mathbb{Z}^3$. The theorems described below are our results. The essence of them is that we understand vectors and twin pairs by putting them into large 3-dimensional cubic lattices.

Theorem 1.5. *Let $x \in \mathbb{Z}^3$ have norm nm^2, where n is square-free. Then there exists an icube (u, v, w) with edge length m such that the corresponding cubic sublattice contains x. If x is primitive, then this cubic lattice is unique, and is given by an Euler matrix $E(\alpha)$, for a quaternion α with integer coefficients.*

The existence part of this result follows from Theorem 4.2 (see Remark 4.3). The uniqueness part is proved at the end of Section 5, but it is also a consequence of Corollary 3.9 and Theorem 4.2.

If (u, v, w) is an icube and $a, b \in \mathbb{Z}$, then $(av + bw, -bv + aw)$ is a twin pair. Theorem 5.4 shows that *we get all twin pairs this way.* To count all twin pairs, the corresponding cubic lattice should be made unique. This is achieved in the same theorem by making the cubic lattice as large as possible, but not necessarily as large as in Theorem 1.5 above. The difficulty is with non-primitive vectors, because there

is no trivial reduction to the primitive case. For example, $3(8,-10,9)$ and $7(4,5,2)$ are twins, and this is explained by the cubic lattice $(u,v,w) = E(2i+j+4k)$, with $a=2$ and $b=1$. Theorem 4.6 shows how a vector in a cubic lattice can be divisible by a prime "unexpectedly". Theorem 5.4 describes, using the language of quaternions, how large this common cubic lattice really is for a given pair of twins. As an application, we count all twin pairs with given norm in Theorem 5.10.

The problem of extending single vectors to twins is more difficult. A consequence of our counting result is that the common norm of twins is always the sum of two squares. The converse, however, is not true, as the example of $(2,2,3)$ shows: its norm is $17 = 1^2+4^2$, but it does not have a twin. The case of primitive vectors is characterized by the following (the proof is at the end of Section 5)

Corollary 1.6. *Using the notation of Theorem 1.5 suppose that x is primitive and $x = au+bv+cw$.*

1. *If none of a, b, c is zero, then x does not have a twin.*
2. *If exactly one of a, b, c is zero, then x has exactly two twins. If, say, $a=0$, then these are $cv-bw$ and its negative.*
3. *If two of a, b, c are zero, then x has exactly four twins, and so is contained in a unique icube. If, say, $a=b=0$, then $c=\pm 1$, $n=1$, and the twins of x are $\pm u$ and $\pm v$. This case happens exactly when the norm of x is a square.*

Definition 1.7. An integer $M>0$ is *twin-complete* if every vector in $\mathbb{Z}^3$ with norm M has a twin, and there is such a vector (that is, M is not of the form $4^n(8k+7)$).

Theorem 1.8. *A positive integer is twin-complete if and only if its square-free part is twin-complete. A positive square-free integer is twin-complete if and only if it can be written as a sum of two squares, but not as a sum of three positive squares.*

We give a complete list of twin-complete numbers modulo the following conjecture.

Conjecture 1.9. The complete list of those square-free numbers that can be written as a sum of two squares, but not as a sum of three positive squares is the following: $\{1,2,5,10,13,37,58,85,130\}$.

Corollary 1.10. *The numbers m^2, $2m^2$, $5m^2$, $10m^2$, $13m^2$, $37m^2$, $58m^2$, $85m^2$, $130m^2$ are twin-complete for every integer $m>0$. If Conjecture 1.9 holds, then there are no other twin-complete numbers.* □

The proof of Theorem 1.8 is in Section 6, where many known results concerning this conjecture are reviewed. The square-free numbers in question form a subset of Euler's *numeri idonei*, and therefore, at most one number can be absent from the list above. If such an integer does exist, it must exceed $2\cdot 10^{11}$ [Wei73], and if it is even, the Generalized Riemann Hypothesis is false [BC00].

Problem 1.11. An avenue for future work is to investigate the *construction, counting, extension* of higher-dimensional icubes.

2. Integral quaternions

In this section we list some basic results and technical facts that we shall use in what follows. The general references about quaternions are [H19], [HW79], and [CS03]. The division ring of all quaternions (with real coefficients) is denoted by $\mathbb{H}$. A quaternion is *pure* if its real part is zero. Quaternions with integer coefficients are called *Lipschitz integral quaternions*. Such a quaternion is *primitive* if its coefficients are relatively prime. Define the special quaternion $\sigma = (1 + i + j + k)/2$.

Proposition 2.1 ([HW79])**.** *We have* $\mathrm{N}(\sigma) = 1$ *and* $\sigma^2 = \sigma - 1$*. Conjugating by* σ *induces a cyclic permutation on* $\{i, j, k\}$ *(see Section 3 for more details).*

Quaternions of the form $a\sigma + bi + cj + dk$ $(a, b, c, d \in \mathbb{Z})$ are called *integral quaternions*, or *Hurwitz integral quaternions* and they form a ring $\mathbb{E}$.

Proposition 2.2. *A quaternion* $\alpha = a + bi + cj + dk$ *belongs to* $\mathbb{E}$ *if and only if the numbers* $2a, 2b, 2c, 2d$ *are rational integers with the same parity. If* α *is such, then* $\mathrm{N}(\alpha) \in \mathbb{Z}$*. A pure integral quaternion has integer coefficients, hence the Euler matrix* $E(\alpha)$*, whose columns are* $\alpha i\,\overline{\alpha}$*,* $\alpha j\,\overline{\alpha}$*,* $\alpha k\,\overline{\alpha}$*, has integer entries.*

The Hurwitz integral quaternions form a maximal order in the rational quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. We shall use the symbol $\mid$ to denote divisibility *on the left* in $\mathbb{E}$.

Proposition 2.3. *An integral quaternion is a unit if and only if its norm is* 1*. These are exactly the* 24 *elements* ± 1*,* $\pm i$*,* $\pm j$*,* $\pm k$*,* $(\pm 1 \pm i \pm j \pm k)/2$*, which form a group under multiplication. Every integral quaternion has a left associate that has integer coefficients (*[HW79]*, p. 305,* [CS03]*, Section 5.2).*

Theorem 2.4. *The ring* $\mathbb{E}$ *is right Euclidean: for every* $\alpha, \beta \in \mathbb{E}$ *with* $\beta \neq 0$*, there exist* $\omega, \rho \in \mathbb{E}$ *such that* $\alpha = \beta\omega + \rho$ *and* $\mathrm{N}(\rho) < \mathrm{N}(\beta)$ *(see Theorem 373 of* [HW79]*).*

Since $\alpha \mapsto \overline{\alpha}$ is an isomorphism between $\mathbb{E}$ and its dual, every assertion that we prove for $\mathbb{E}$ remains true if we replace "left" with "right" and vice versa. As $\mathbb{E}$ is left Euclidean, every element can be written as a product of irreducible quaternions. This decomposition is unique in a certain sense (see [CS03], Section 5.2).

We shall need the following two technical lemmas.

Lemma 2.5. *Suppose that* $\alpha \in \mathbb{E}$ *and* $p \in \mathbb{Z}$ *is a prime such that* $p \mid \mathrm{N}(\alpha)$ *but* p *does not divide* α*. Then* α *can be written as* $\pi\alpha'$*, where* $\mathrm{N}(\pi) = p$*. This* π *is uniquely determined up to right association.*

An element π *is a left divisor of* α *with norm* p *if and only if* π *is the generator of the right ideal* $(\alpha, p)_r$*.*

Proof. The fact that α is left divisible by a prime π of norm p, with the additional property $(\pi)_r = (\alpha, p)_r$, follows easily from Theorem 2 in Section 5.2 of [CS03]. (Note that that argument only uses the hypothesis that p does not divide α, not

the primitivity of α.) Suppose that π_1 is also left divisor of α with norm p. Then α and $p = \pi_1\overline{\pi_1}$ are in $(\pi_1)_r$, so $(\pi)_r = (\alpha, p)_r \subseteq (\pi_1)_r$. Thus, π_1 divides π on the right, and as they have the same norm, they are right associates, implying also that $(\pi_1)_r = (\pi)_r = (\alpha, p)_r$. □

Lemma 2.6. *Suppose that $\theta, \eta, \pi \in \mathbb{E}$, such that $\mathrm{N}(\pi) = p$ is a prime in $\mathbb{Z}$. If $\pi \mid \theta$, $p \mid \overline{\theta}\eta$ but p does not divide θ, then $\pi \mid \eta$.*

Proof. By Lemma 2.5, $(p, \theta)_r = (\pi)_r$, that is, $\pi = \theta\tau_1 + p\tau_2$, for some $\tau_1, \tau_2 \in \mathbb{E}$. Hence, $\overline{\pi}\eta = \overline{\tau_1}\overline{\theta}\eta + p\overline{\tau_2}\eta$, and as p divides $\overline{\theta}\eta$, we get that $p \mid \overline{\pi}\eta$. Using $p = \overline{\pi}\pi$, this shows that $\pi \mid \eta$. □

Theorem 2.7. *An integral quaternion is irreducible in the ring $\mathbb{E}$ if and only if its norm is a prime in $\mathbb{Z}$ (see Theorem 377 of* [HW79]*). The only elements of $\mathbb{E}$ whose norm is 2 are $\lambda = 1 + i$ and its left associates. If $p > 2$ is a prime in $\mathbb{Z}$, then there exist exactly $24(p + 1)$ integral quaternions whose norm is p (see the note right after the proof of Theorem 3 in Section 5.3 of* [CS03]*).*

Corollary 2.8. *The number of integral quaternions with norm n is 24 times the sum of positive odd divisors of n.*

Lemma 2.9. *Let $p \in \mathbb{Z}$ be a prime and $\ell \geq 0$. Suppose that $\pi_1 \in \mathbb{E}$ is fixed and has norm p. Consider all integer quaternions α such that $\mathrm{N}(\alpha) = p^\ell$ and $\alpha\pi_1$ is not divisible by p. Then the number of such α is $24p^\ell$.*

Proof. We do induction on ℓ. If $\ell = 0$, then the statement is trivial, since the number of units is 24. Suppose that p does not divide α. The dual of Lemma 2.5 shows that α can be written as $\alpha_2\pi_2$, with $\mathrm{N}(\pi_2) = p$, where α_2 is unique up to right association, and π_2 is unique up to left association. Apply Lemma 2.6 for $\theta \mapsto \overline{\alpha}$, $\eta \mapsto \pi_1$, and $\pi \mapsto \overline{\pi_2}$. We get that if $\alpha\pi_1$ is divisible by p, then π_2 and $\overline{\pi_1}$ are left associates. Conversely, if π_2 and $\overline{\pi_1}$ are left associates, then clearly $p \mid \alpha\pi_1$.

By Theorem 2.7, the number of elements of norm p up to left association is $p + 1$. So π_2 can be chosen p ways, and by the induction assumption, α_2 can be chosen $24p^{\ell-1}$ ways for every given π_2. Thus, α can be chosen $24p^{\ell-1}p$ ways. □

3. Integral Euler matrices

Our goal in this section is to characterize (in Theorem 3.3) all Euler matrices $E(\alpha)$ with integer entries (called *integral Euler matrices*) in terms of the corresponding quaternion α. Sárközy's Theorem 1.2 is obtained as Corollary 3.9

First, we demonstrate how to permute the columns of an Euler matrix by changing its generating quaternion. By Theorem 1.1, $E(\alpha)$ is the matrix of $R(\alpha) : \beta \mapsto \alpha\beta\,\overline{\alpha}$, hence $E(\alpha\varepsilon) = E(\alpha)E(\varepsilon)$. The map $R(\alpha)$ is always orientation-preserving, but the map corresponding to an icube (as a matrix) may not be. This problem is averted by taking the negative of an odd number of columns.

Proposition 3.1 (cf. [CS03], Section 3.5)**.** *Let ε be*

(A) *σ or σ^{-1}, where $\sigma = (1+i+j+k)/2$. Then $R(\varepsilon)$ is the rotation of $\mathbb{R}^3$ about the vector $i+j+k$ by an angle of $\pm 120^\circ$ (thus cyclically permuting the three coordinate axes). Therefore, $E(\alpha\varepsilon)$ is obtained from $E(\alpha)$ by applying a cyclic permutation to the columns.*

(B) *$(1 \pm i)/\sqrt{2}$. Then $R(\varepsilon)$ is the rotation about the unit vector $i \in \mathbb{Z}^3$ by an angle of $\pm 90^\circ$ (interchanging the other two coordinate axes). Therefore, $E(\alpha\varepsilon)$ is obtained from $E(\alpha)$ by switching the last two columns and taking the negative of one. A similar statement holds for $(1 \pm j)/\sqrt{2}$ and $(1 \pm k)/\sqrt{2}$.*

(C) *$\pm i$. Then $R(\varepsilon)$ is the half turn (that is, 180° rotation) about the unit vector $i \in \mathbb{Z}^3$ (fixing all coordinate axes). Therefore, $E(\alpha\varepsilon)$ is obtained from $E(\alpha)$ by taking the negative of the last two columns. A similar statement holds for $\pm j$ and $\pm k$. This transformation is the square of the one described in (B).*

Every non-identical permutation of the columns of $E(\alpha)$ can be obtained by one of the above modifications of α, but in case of an odd permutation one of the columns changes its sign. One can also change the sign of any two columns. □

Before proceeding, let us review the action of these isometries on $\mathbb{R}^3$.

Proposition 3.2 (cf. [CS03], Section 3.5)**.** *Denote by H the group of units of $\mathbb{E}$ (see Proposition 2.3), set $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ and let G be the subgroup of the multiplicative group of $\mathbb{H}$ generated by H and $(1+i)/\sqrt{2}$. Then G contains all the isometries investigated in Proposition 3.1. The group G has 48 elements.*

The element σ has order 6. The rotation $R(\sigma)$ maps $\eta = ai+bj+ck$ to $ci+aj+bk$, so it permutes the components cyclically.

The element $(1+i)/\sqrt{2}$ has order 8. The corresponding rotation $R\big((1+i)/\sqrt{2}\big)$ maps η to $ai-cj+bk$. The square of this rotation is $R(i)$, mapping η to $ai-bj-ck$.

In general, G acts on the set of pure quaternions via the rotations $R(\rho)$ with $\rho \in G$. The orbit of η under Q consists of η, $-ai-bj+ck$, $-ai+bj-ck$, and $+ai-bj-ck$. If we disregard the signs, then every other element of H induces a fixed point free permutation on the components of η. □

Theorem 3.3. *$E(\alpha)$ is a primitive integral Euler matrix if and only if the non-zero quaternion α belongs to one of the following three types.*

(1) *α is a primitive Lipschitz integral quaternion with an odd norm.*

(2) *$\alpha = \beta/\sqrt{2}$, where β is a primitive Lipschitz integral quaternion such that $\mathrm{N}(\beta) \equiv 2\ (4)$, or equivalently: exactly two components of β are odd.*

(3) *$\alpha = \beta/2$, where β is a primitive Lipschitz integral quaternion such that $\mathrm{N}(\beta) \equiv 4\ (8)$, or equivalently: all four components of β are odd (so α is a Hurwitz integral quaternion).*

In all cases $\mathrm{N}(\alpha)$ *is an odd integer. Each column and each row of* $E(\alpha)$ *contains exactly one odd entry. The number of odd entries in the main diagonal in types* (1), (2), (3) *are* 3, 1, 0, *respectively.*

The proof requires four lemmas, whose proofs are elementary calculations.

Lemma 3.4. *If* β *is a primitive Lipschitz integral quaternion, then* $\mathrm{N}(\beta)$ *cannot be divisible by* 8. *It is congruent to* 2 *modulo* 4 *if and only if* β *has exactly two odd components, and is congruent to* 4 *modulo* 8 *if and only if all components of* β *are odd.* □

Lemma 3.5. *If* $E(\alpha)$ *is a primitive integral Euler matrix, then* $\mathrm{N}(\alpha)$ *is an odd integer. Each column and each row contains exactly one odd entry.* □

Lemma 3.6. *If the quaternion* $\alpha = (m + ni + pj + qk)/2$ *belongs to class* (3) *of Theorem 3.3, then either* $\alpha\sigma$ *or* $\alpha\sigma^{-1}$ *is a quaternion of class* (1). □

Lemma 3.7. *Every quaternion* $\alpha = (m + ni + pj + qk)/\sqrt{2}$ *of class* (2) *can be multiplied on the right by a suitable unit* $(1 + u)/\sqrt{2}$ *to transform it to a quaternion of class* (1), *where* $u \in \{i, j, k\}$. □

Proof of Theorem 3.3. Put $\alpha = m + ni + pj + kq$ with real numbers m, n, p, q, and assume that the Euler matrix $E(\alpha)$ given in Theorem 1.1 has integral entries and is primitive. By Lemma 3.5, $\mathrm{N}(\alpha) = m^2 + n^2 + p^2 + q^2$ is an integer, and the diagonal elements of $E(\alpha)$ are also integers. Taking linear combinations of these quadratic forms, we get that $4m^2$, $4n^2$, $4p^2$, and $4q^2$ are all integers. By adding and subtracting symmetric off-diagonal elements, we obtain that $4mn$, $4mp$, $4mq$, $4np$, $4nq$, and $4pq$ are integers as well. Therefore, the square-free parts of the non-zero numbers among $4m^2, 4n^2, 4p^2$, and $4q^2$ are the same. Denote this common square-free part by r. The quaternion $\alpha = m + ni + pj + qk$ can be written uniquely in the form

$$\alpha = \frac{k\sqrt{r}}{2}(a + bi + cj + dk), \tag{3.8}$$

where $k \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$, $(a, b, c, d) = 1$. Since the matrix $E(\alpha)$ is primitive, neither k nor the square-free r can have any odd prime divisor, and k (as a power of 2) cannot be greater than 2. Hence, both k and r are elements of the set $\{1, 2\}$, but $k = r = 2$ violates primitivity of $E(\alpha)$. Thus, we are left with the cases

(*a*) $k = 2$, $r = 1$;
(*b*) $k = 1$, $r = 2$;
(*c*) $k = r = 1$.

These correspond exactly to the cases listed as (1), (2), and (3) in Theorem 3.3. Lemma 3.5 shows that $\mathrm{N}(\alpha)$ is an odd integer. Therefore, Lemma 3.4 finishes the proof of one implication of the theorem.

Assume now that the quaternion α is one of the types (1)–(3) in Theorem 3.3. We want to show that $E(\alpha)$ is a primitive integer matrix. By Lemmas 3.6 and 3.7, there exists a suitable quaternion $\varepsilon \in \mathbb{H}$ with $\mathrm{N}(\varepsilon) = 1$ such that $\alpha\varepsilon$ is of class (1), and by Proposition 3.1, we see that $E(\alpha\varepsilon) = E(\alpha)E(\varepsilon)$ is a primitive integral matrix if and only if $E(\alpha)$ is.

We show that $E(\alpha\varepsilon)$ is primitive. Since $\mathrm{N}(\alpha\varepsilon)$ is odd by assumption, the entries in the main diagonal of $E(\alpha\varepsilon)$ are odd. Suppose that an odd rational prime t divides all entries of $E(\alpha\varepsilon)$. Let $\alpha\varepsilon = m + ni + pj + qk$. The simple calculation preceding (3.8) shows that t divides the numbers $4m^2, 4n^2, 4p^2$, and $4q^2$, violating the primitivity of $\alpha\varepsilon$. Thus, $E(\alpha\varepsilon) = E(\alpha)E(\varepsilon)$ is indeed a primitive integer matrix.

We now show the last statement of the theorem. If α belongs to type (1), then, as we saw above, the entries in the main diagonal are odd, while the other entries are clearly even. Quaternions of class (2) are handled by Lemma 3.7, and these correspond to the interchange of two columns by (B) of Proposition 3.1. The type (3) case is handled by Lemma 3.6 and yields a cyclic fixed point free permutation of the columns, by (A) of Proposition 3.1. This completes the proof of Theorem 3.3. □

Corollary 3.9. *Consider a primitive icube as the columns of a matrix M. Then there exists a Lipschitz integral quaternion α such that, by permuting the columns of $E(\alpha)$ and changing the sign of the last column if necessary, we get M.*

Proof. Change the sign of the last column if and only if M is orientation-reversing. The new M can be written as $M = E(\alpha)$, for some quaternion α (with real coefficients) by Theorem 1.1. This α belongs to one of the three types listed in Theorem 3.3. Modify α using Proposition 3.1 so that the odd entries move to the main diagonal. Then we get a Lipschitz integral quaternion by the last statement of Theorem 3.3. If this transformation changes the sign of a column other than what was initially the third, then use Proposition 3.1 to change the sign of two columns to what they were originally. □

4. A representation of pure integral quaternions

In this section we decompose single pure quaternions. Geometrically, this means that we find a large cubic lattice that contains the corresponding vector. Algebraically, a cubic lattice is the subgroup of all quaternions $\delta = \alpha\beta\,\overline{\alpha}$, where α is a fixed Hurwitz integral quaternion and β runs over all pure integral quaternions. The generating icube is given by $\alpha i\,\overline{\alpha}$, $\alpha j\,\overline{\alpha}$, $\alpha k\,\overline{\alpha}$.

The primitive case is easier, and is handled by Theorem 4.2. This already implies Theorem 1.4, and the existence statement of Theorem 1.5. Theorem 4.6 explains how a vector in a cubic lattice can be divisible by a prime "unexpectedly". This will be used in the characterization of twin-complete numbers, and is also sufficient to obtain a classical result about counting all vectors of a given length (Theorem 4.8, Corollary 4.9).

The results in this section are closely related to those in [Pal40], but that paper deals primarily with Lipschitz integral quaternions.

Lemma 4.1. *Let $\delta \in \mathbb{E}$ be a pure quaternion and $p \in \mathbb{Z}$ a prime such that $p^2 \mid \mathrm{N}(\delta)$ but p does not divide δ. Then there exists an element $\pi \in \mathbb{E}$ whose norm is p such that $\delta = \pi\delta_1\overline{\pi}$, for some $\delta_1 \in \mathbb{E}$.*

Proof. By Lemma 2.5, we get that $\delta = \pi\delta_2$, for some $\pi, \delta_2 \in \mathbb{E}$ such that $\mathrm{N}(\pi) = p$. Then $\mathrm{N}(\delta) = p\,\mathrm{N}(\delta_2)$. Hence, p divides $\mathrm{N}(\delta_2)$ but p clearly does not divide δ_2. By the dual of Lemma 2.5, we obtain an element $\pi_1 \in \mathbb{E}$ with norm p such that $\delta_2 = \delta_3\pi_1$. Hence, $\delta = \pi\delta_3\pi_1$. Taking conjugates, we get $\overline{\delta} = \overline{\pi_1}\overline{\delta_3}\overline{\pi}$; however, δ is a pure quaternion, hence $\overline{\delta} = -\delta$. Therefore, δ is divisible by π and by $\overline{\pi_1}$ on the left. By the uniqueness statement of Lemma 2.5, we get that π and $\overline{\pi_1}$ are right associates. Thus, $\delta = \pi\delta_3\pi_1$ can indeed be written as $\pi\delta_1\overline{\pi}$. □

Theorem 4.2. *Let $\delta \in \mathbb{E}$ be a pure quaternion with $\mathrm{N}(\delta) = nm^2$. Suppose that no integer prime divisor of m divides δ. Then δ can be written as $\alpha\beta\,\overline{\alpha}$, for some $\alpha, \beta \in \mathbb{E}$ such that $\mathrm{N}(\alpha) = m$ and $\mathrm{N}(\beta) = n$. Here α is uniquely determined, that is, any two such elements α are right associates of each other and the corresponding elements β are group-conjugates of each other via a unit of $\mathbb{E}$. If $n = 1$, then β can be chosen freely to be any element of $\{\pm i, \pm j, \pm k\}$.*

Proof. The existence of α and β is easily proven by induction on m: apply Lemma 4.1 successively for each of the prime divisors of m.

For the uniqueness assume that $\delta = \alpha_1\beta_1\overline{\alpha_1} = \alpha_2\beta_2\overline{\alpha_2}$. We use induction on m again. If $m = 1$, then α_1 and α_2 are units, so they are right associates, and the unit $\varepsilon = \alpha_2^{-1}\alpha_1$ satisfies $\varepsilon\beta_1\varepsilon^{-1} = \beta_2$. If $m > 1$, then let $p \in \mathbb{Z}$ be a prime divisor of m. Apply Lemma 2.5 to get $\pi_1, \pi_2 \in \mathbb{E}$, with $\pi_1 \mid \alpha_1$ and $\pi_2 \mid \alpha_2$. Then π_1 and π_2 divide δ on the left, and the uniqueness statement of Lemma 2.5 implies that π_1 and π_2 are right associates. Thus, if $\pi_2 = \pi_1\varepsilon$, $\alpha_1 = \pi_1\alpha_3$ and $\alpha_2 = \pi_2\alpha_4$, then $\delta' = \alpha_3\beta_1\,\overline{\alpha_3} = (\varepsilon\alpha_4)\beta_2\,\overline{\varepsilon\alpha_4}$. By the induction hypothesis, α_3 and $\varepsilon\alpha_4$ are right associates. Similarly, we see that $\alpha_1 = \pi_1\alpha_3$ and $\alpha_2 = \pi_1\varepsilon\alpha_4$ are also right associates.

If $n = 1$, then β is a unit in $\mathbb{E}$. Since β is a pure quaternion, it is contained in $\{\pm i, \pm j, \pm k\}$. These six elements are group-conjugates of each other via a unit by Proposition 3.2. Therefore, by taking a right associate of α, we may choose any of them to be β. □

Remark 4.3. Theorem 4.2 implies Theorem 1.4, and the existence statement of Theorem 1.5. (The uniqueness part of Theorem 1.5 clearly follows from Theorem 4.2 and Corollary 3.9, but we give a "pure number-theoretic" proof in Section 5.)

Proof. Let u be a primitive vector and denote by δ the corresponding pure quaternion. Decompose δ using Theorem 4.2 as $\delta = \alpha\beta\,\overline{\alpha}$ with $\mathrm{N}(\alpha) = m$. Then the cubic lattice

corresponding to α has edge length m and contains u. This yields the existence statement of Theorem 1.5.

If the length if u is an integer, then $n = 1$ and we may assume that $\beta = i$. Then $\alpha j\,\overline{\alpha}$ and $\alpha k\,\overline{\alpha}$ extend u to an icube, proving Theorem 1.4 in the primitive case. The general case obviously follows from this. □

Lemma 4.4. *Let $\beta, \beta_1 \in \mathbb{E}$ be pure quaternions, each of norm n. If $\beta + \beta_1 \neq 0$, then we have $(\beta + \beta_1)\beta(\beta + \beta_1)^{-1} = \beta_1$.*

Proof. The proof is a straightforward calculation using $\beta^2 = \beta_1^2 = -n$. Instead of presenting it, we explain this formula geometrically. Since $\gamma = \beta + \beta_1$ is a nonzero pure quaternion, conjugation by γ acts on $\mathbb{R}^3$ as half turn about the line through γ, which clearly takes β to β_1. □

Lemma 4.5. *Let $\pi, \beta \in \mathbb{E}$ such that β is a pure quaternion and $p = \mathrm{N}(\pi) > 2$ is a prime in $\mathbb{Z}$. Then $\pi\beta\pi^{-1} \in \mathbb{E}$ if and only if there exists an integer $h \in \mathbb{Z}$ such that $\overline{\pi} \mid h + \beta$.*

Proof. Suppose that $\overline{\pi} \mid h + \beta$, that is, $\overline{\pi}\tau = h + \beta$, for some $\tau \in \mathbb{E}$. Then

$$p\tau\overline{\pi} = \pi\overline{\pi}\tau\overline{\pi} = \pi h\overline{\pi} + \pi\beta\,\overline{\pi} = ph + \pi\beta\,\overline{\pi}\,.$$

Hence, $p \mid \pi\beta\,\overline{\pi}$, which shows that $\pi\beta\pi^{-1} = (\pi\beta\,\overline{\pi})/p$ is indeed an integral quaternion.

To prove the converse, set $\beta_1 = \pi\beta\pi^{-1}$ and $\tau = \beta + \beta_1$. We can assume that π does not divide τ on the left, as we now show. Let

$$\beta_2 = (i\pi)\beta(i\pi)^{-1} = i\beta_1 i^{-1}\,,$$

which is still an integral quaternion. It is clearly sufficient to prove that $\overline{i\pi} \mid h + \beta$, so we can work with $i\pi$ instead of π in the argument below. If, however, both π and $i\pi$ are "bad", that is, $\pi \mid \tau = \beta + \beta_1$ and $i\pi \mid \beta + \beta_2$, then $\pi \mid i^{-1}\beta i + \beta_1$, which implies $\pi \mid \beta - i^{-1}\beta i$. Put $\beta = ai + bj + ck$. Then $\beta - i^{-1}\beta i = 2(bj + ck)$. If $j\pi$ and $k\pi$ are also "bad", then π divides $2(ai + ck)$ and $2(ai + bj)$ as well. Taking norms, we get, using $\mathrm{N}(\pi) = p > 2$, that p divides $a^2 + b^2$, $a^2 + c^2$, and $b^2 + c^2$. Thus, p divides a, b, c, and, finally, p divides β. Therefore, $\overline{\pi} \mid h + \beta$, for $h = 0$, and we are done in this case. We can then indeed assume that π does not divide τ on the left.

Lemma 4.4 implies that $\tau\beta\tau^{-1} = \beta_1 = \pi\beta\pi^{-1}$, so $\tau^{-1}\pi$ centralizes β. Let $d = \mathrm{N}(\tau)$. Then $d\tau^{-1}\pi = \overline{\tau}\pi$ centralizes β as well. The centralizer of β consists of elements $r + s\beta$, where $r, s \in \mathbb{R}$. This set is closed under conjugation, since β is a pure quaternion, and therefore, contains $\overline{\overline{\tau}\pi} = \overline{\pi}\tau$. If we write $\overline{\pi}\tau = u + v\beta$, where u and v are real, and $\beta = d\beta'$, where $d \in \mathbb{Z}$ and β' is primitive, then $2u$ and $2vd$ are integers. (We need the factor 2, because the integral quaternion $\overline{\pi}\tau$ need not have integer coefficients).

We now show that p does not divide $2vd$. Suppose it does. Taking norms, we get that $\mathrm{N}(\overline{\pi}) = p \mid 4\,\mathrm{N}(u + v\beta) = (2u)^2 + (2vd)^2\,\mathrm{N}(\beta')$, so $p \mid 2u$. Thus, either $u + v\beta$ has integer coefficients, which are divisible by p, or $2u + 2v\beta$ has odd integer coefficients

that are divisible by p. Since $p \neq 2$, we have $u' + v'\beta = (u + v\beta)/p \in \mathbb{E}$ in either case. Then $\overline{\pi}\tau = u + v\beta = p(u' + v'\beta) = \overline{\pi}\pi(u' + v'\beta)$, and $\tau = \pi(u' + v'\beta)$, contradicting our assumption that π does not divide τ on the left. Therefore, we have that p does not divide $2vd$.

Let x, y be integers such that $(2vd)x + yp = 1$. Then

$$\overline{\pi} \mid 2x(u + vd\beta') = x(2u) + (1 - yp)\beta' .$$

Since $\overline{\pi} \mid p$, we get that $\overline{\pi} \mid x(2u) + \beta'$ and take $h = x(2u)d$. □

Theorem 4.6. *Suppose that $\alpha, \beta \in \mathbb{E}$ such that β is a pure quaternion and $p \in \mathbb{Z}$ is a prime. Then $p \mid \alpha\beta\,\overline{\alpha}$ if and only if one of the following cases holds.*

1. *p divides α or β.*
2. *$p = 2$ and does not divide α, β, but divides $\mathrm{N}(\alpha)$.*
3. *$p > 2$ and does not divide α, β, but divides $\mathrm{N}(\alpha)$, and there exists a right divisor π of α with norm p and an integer $h \in \mathbb{Z}$ such that $\overline{\pi} \mid h + \beta$.*

In particular, every prime divisor of $\alpha\beta\,\overline{\alpha}$ divides either β or $\mathrm{N}(\alpha)$.

Proof. If (1) holds, then clearly $p \mid \alpha\beta\,\overline{\alpha}$. If (2) holds, then the dual of Lemma 2.5 shows that α is right divisible by $1 + i$ (since this is the only element in $\mathbb{E}$ of norm 2 up to left association), and Proposition 3.2 yields that $(1 + i)\beta\,\overline{1 + i}$ is divisible by 2. Finally, if (3) holds, then $p \mid \pi\beta\,\overline{\pi}$ by Lemma 4.5. This proves one direction of the theorem.

Now assume that $p \mid \alpha\beta\,\overline{\alpha}$ but α and β are not divisible by p. If p does not divide $\mathrm{N}(\alpha)$, then we have $p \mid \overline{\alpha}(\alpha\beta\,\overline{\alpha})\alpha = \mathrm{N}(\alpha)^2\beta$. Hence, $p \mid \beta$, which is a contradiction. Therefore, we may assume that we are in case (3), that is, $p > 2$ and $p \mid \mathrm{N}(\alpha)$. We proceed by induction on $\mathrm{N}(\alpha)$. By the dual of Lemma 2.5, $\alpha = \alpha_1\pi$ for some $\alpha_1, \pi \in \mathbb{E}$, with $\mathrm{N}(\pi) = p$. We show that $\beta_1 = \pi\beta\,\overline{\pi}$ is divisible by p. Then we are clearly done by Lemma 4.5.

Suppose β_1 is not divisible by p. Apply the induction hypothesis to $\alpha_1\beta_1\,\overline{\alpha_1}$ (which is equal to $\alpha\beta\,\overline{\alpha}$). We must be in case (3), since $p > 2$ and p does not divide both α_1 and β_1. Therefore, there exists a right divisor π_1 of α_1 of norm p and an integer h_1 such that $\overline{\pi_1} \mid h_1 + \beta_1$. Taking norms, we see that $p = \mathrm{N}(\overline{\pi_1}) \mid \mathrm{N}(h_1 + \beta) = h_1^2 + \mathrm{N}(\beta_1)$; however, $\mathrm{N}(\beta_1) = p^2\,\mathrm{N}(\beta)$ is divisible by p, so $p \mid h_1$, and therefore, $\overline{\pi_1} \mid \beta_1$. Since β_1 is not divisible by p, the uniqueness part of Lemma 2.5 shows that $\overline{\pi_1}$ and π are right associates. This implies α is divisible on the right by $\pi_1\overline{\pi_1} = p$, contradicting our assumptions. □

Proposition 4.7. *Suppose that $\beta \in \mathbb{E}$ is a pure quaternion and p is a prime not dividing β. Denote by e the number of different quaternions of the form $\varepsilon\beta\varepsilon^{-1}$, where ε runs over the units of $\mathbb{E}$. Consider all quaternions α whose norm is p^ℓ, with some fixed $\ell > 0$. If $p > 2$, then the number of quaternions of the form $\alpha\beta\,\overline{\alpha}$ that are not divisible by p is*

(1) ep^ℓ, *if* $p \mid \mathrm{N}(\beta)$;
(2) $e(p^\ell - p^{\ell-1})$, *if* $-\mathrm{N}(\beta)$ *is a quadratic residue mod* p;
(3) $e(p^\ell + p^{\ell-1})$ *otherwise.*

If $p = 2$, *then this number is* 0.

Proof. If $p = 2$ (and $\ell > 0$), then Theorem 4.6 shows that $\alpha\beta\,\overline{\alpha}$ is divisible by p, so suppose that p is odd. We call a pair (α_1, β_1) "good", if $\alpha_1 \in \mathbb{E}$ with $\mathrm{N}(\alpha_1) = p^\ell$ and there is a unit $\varepsilon \in \mathbb{E}$ such that $\beta_1 = \varepsilon^{-1}\beta\varepsilon$, and p does not divide $\alpha_1\beta_1\,\overline{\alpha_1}$. By the uniqueness part of Theorem 4.2, every element $\alpha_1\beta_1\,\overline{\alpha_1}$ is given by exactly 24 pairs. Therefore, it is sufficient to count the good pairs for any given β_1.

Let (α_1, β_1) be a good pair. Then clearly α_1 is not divisible by p, so we can write $\alpha_1 = \alpha_2\pi_2$ by Lemma 2.5, where π_2 of norm p is uniquely determined up to left association. Theorem 4.6 shows that $\alpha_1\beta_1\overline{\alpha_1}$ is divisible by p if and only if $\overline{\pi_2}$ divides $h + \beta_1$, for some integer h (assuming that α_1 is not divisible by p). We now count the number of such quaternions π_2.

Clearly, $\overline{\pi_2} \mid h + \beta_1$ implies $\mathrm{N}(\pi_2) = p \mid \mathrm{N}(h + \beta_1) = h^2 + \mathrm{N}(\beta_1)$. This means that either $p \mid \mathrm{N}(\beta_1)$ or $-\mathrm{N}(\beta_1)$ is a quadratic residue mod p. Hence, in case (3) above there is no such π_2. Since p does not divide β_1, it does not divide $h + \beta_1$. Thus, by the uniqueness statement of Lemma 2.5, there is exactly one left divisor $\overline{\pi_2}$ up to right association with norm p of any given $h + \beta_1$ for which $p \mid h^2 + N(\beta_1)$, and π_2 is unique up to left association. Clearly, the numbers h_1 and h_2 yield the same $\overline{\pi_2}$ if and only if $h_1 \equiv h_2\ (p)$. If $p \mid \mathrm{N}(\beta_1)$, then $h = 0$ is the only possibility. This yields one "bad" value for π_2 up to left association. Otherwise, there are exactly two values $1 \le h \le p-1$ such that $p \mid h^2 + \mathrm{N}(\beta_1)$ (since p is an odd prime, assuming, of course, that $-\mathrm{N}(\beta_1)$ is a quadratic residue mod p). So, in this case there are two "bad" values for π_2 up to left association.

By Theorem 2.7, the number of possible choices for π_2 is $p+1$ up to left association. Thus, for every given β_1, the number of good values for π_2 is p, $p-1$ and $p+1$, respectively, corresponding to cases (1), (2) and (3) in the claim. If π_2 is fixed, then the number of choices for α_2 so that α_1 is not divisible by p is, by Lemma 2.9, $24p^{\ell-1}$. Since the number of possible β_1 is e, we get the result. □

In the theorem below, $(-n/p)$ denotes the Legendre symbol (which is defined to be 0 if $p \mid n$).

Theorem 4.8. *Suppose that* $m, n \ge 1$ *are integers and* n *is square-free. If* m *is odd, then the number* $p(nm^2)$ *of primitive vectors* (x, y, z) *whose norm is* nm^2 *is*

$$p(nm^2) = p(n) \prod \left(p^\ell - (-n/p)p^{\ell-1}\right),$$

where p^ℓ *runs over the prime powers in the canonical form of* m. *If* m *is even, then* $p(nm^2) = 0$.

Proof. We proceed by induction on the number of prime divisors of m. Suppose that $m = p^\ell m_1$, where p does not divide m_1. Theorem 4.2 implies that the pure quaternion $\delta = xi + yj + zk$ corresponding to (x, y, z) can be represented as $\alpha\beta\,\overline{\alpha}$, where $\mathrm{N}(\alpha) = p^\ell$.

Theorem 4.6 shows that if β is primitive, then the only possible prime divisor of $\alpha\beta\,\overline{\alpha}$ is p, and if $p = 2$ and $\ell > 0$, then $\alpha\beta\,\overline{\alpha}$ is not primitive, because it is divisible by 2. Thus, if $p > 2$, then $\alpha\beta\,\overline{\alpha}$ is primitive if and only if β is primitive and $\alpha\beta\,\overline{\alpha}$ is not divisible by p. The formula for $p(nm^2)$ then follows clearly from Proposition 4.7. □

The following is a well-known formula (see (29) in [Pal40]), and follows with some effort from Theorem 4.8.

Corollary 4.9. *Suppose that $m, n \geq 1$ are integers and n is square-free. The number $s(nm^2)$ of all vectors of norm nm^2 is*

$$s(nm^2) = s(n) \prod \left(\sigma(p^\ell) - (-n/p)\sigma(p^{\ell-1}) \right),$$

where p^ℓ runs over the odd prime powers in the canonical form of m and $\sigma(s)$ denotes the sum of positive divisors of any integer s.

5. A parameterization of twin pairs

Theorem 5.4 is our main characterization of twins. In Theorem 5.10, we count twin pairs with a given norm. Finally, we deal with the problem of extension. In Corollary 5.11, we show that each pair of twins whose length is an integer extends to an icube. Then, at the end of the section, we prove Theorem 1.5 and Corollary 1.6.

Recall that every vector $v = (v_1, v_2, v_3) \in \mathbb{R}^3$ is identified with the pure quaternion $V(v) = v_1 i + v_2 j + v_3 k$.

Proposition 5.1. *Two vectors v and w in $\mathbb{Z}^3$ are twins if and only if $\theta = V(v)$ and $\eta = V(w)$ satisfy the following conditions.*

1. *θ and η are nonzero pure quaternions;*
2. *$\mathrm{N}(\theta) = \mathrm{N}(\eta)$;*
3. *$\theta\eta$ is also a pure quaternion;*
4. *θ and η have integer coefficients.*

We call a pair of such quaternions (θ, η) a twin pair.

Proof. It is easy to verify that the real part of $V(v)V(w)$ equals the negative of the dot product of v and w, and the pure quaternion part of $V(v)V(w)$ corresponds to the cross product of v and w. □

We now translate the construction of twin pairs given in the Introduction. Denote by (u, v, w) the columns of an Euler matrix given by $\alpha \in \mathbb{E}$. By Proposition 2.2, $\mathrm{N}(\alpha)$ and the components of (u, v, w) are integers. Let $z = a + bi \in \mathbb{G}$ (the ring of Gaussian integers). Then $E(\alpha)$ maps i to $V(u)$, j to $V(v)$, and k to $V(w)$. It maps

the twin quaternions $zj = aj + bk$ and $zk = ak - bj$ to $\alpha zj\,\overline{\alpha}$ and $\alpha zk\,\overline{\alpha}$, respectively, which correspond to the twin pair $(av + bw, -bv + aw)$.

Definition 5.2. We say that (θ, η) is *parameterized* by the pair $(\alpha, z) \in \mathbb{H} \times \mathbb{C}$ if $\theta = \alpha zj\,\overline{\alpha}$ and $\eta = \alpha zk\,\overline{\alpha}$. Two pairs in $(\alpha_1, z_1) \in \mathbb{H} \times \mathbb{C}$ and $(\alpha_2, z_2) \in \mathbb{H} \times \mathbb{C}$ are *equivalent* if they parameterize the same (θ, η), that is, if $\alpha_1 z_1 j\,\overline{\alpha_1} = \alpha_2 z_2 j\,\overline{\alpha_2}$ and $\alpha_1 z_1 k\,\overline{\alpha_1} = \alpha_2 z_2 k\,\overline{\alpha_2}$.

Proposition 5.3. *Suppose that (θ, η) is parameterized by a pair $(\alpha, z) \in \mathbb{H} \times \mathbb{C}$. Then $\theta\eta = \mathrm{N}(\alpha)\,\mathrm{N}(z)\alpha i\,\overline{\alpha}$, so θ and η satisfy* (1)–(3) *of Proposition 5.1. If $\alpha \in \mathbb{E}$ and $z \in \mathbb{G}$, then θ and η have integer coefficients and are twins.*

Proof. Note that $\alpha^{-1} = \overline{\alpha}/\,\mathrm{N}(\alpha)$ and $x \mapsto \alpha x \alpha^{-1}$ is an automorphism of the division ring $\mathbb{H}$. Therefore, $\theta\eta = \mathrm{N}(\alpha)\alpha zjzk\,\overline{\alpha}$; however, $zjzk = zjzj^{-1}jk = z\overline{z}i$, so the quaternion $\theta\eta = \mathrm{N}(\alpha)\,\mathrm{N}(z)\alpha i\,\overline{\alpha}$ is pure. □

Theorem 5.4. *The characterization of twin quaternions is given by the following.*

1. *The quaternions θ and η are twins if and only if (θ, η) is parameterized by a pair in $\mathbb{E} \times \mathbb{G}$ (whose components are nonzero).*
2. *Every pair in $\mathbb{E} \times \mathbb{G}$ is equivalent to a pair, where the second component is* square-free *in $\mathbb{G}$.*
3. *Let $(\alpha_1, z_1), (\alpha_2, z_2) \in \mathbb{E} \times \mathbb{G}$ be such that both z_1 and z_2 are square-free. Then these pairs are equivalent if and only if there exists a unit $\rho \in \mathbb{G}$ (that is, an element of $\{\pm 1, \pm i\}$) such that $\alpha_2 = \alpha_1\rho$ and $z_2 = \rho^2 z_1$.*
4. *The length of the twins θ and η is an integer if and only if in the parameterization (α, z) of (θ, η), where z is square-free, $z \in \mathbb{G}$ is either real or pure imaginary.*

The condition that z is square-free expresses the fact that the cubic lattice given by α is as large as possible. We prove this theorem through a series of assertions.

Lemma 5.5. *Suppose that $\theta, \eta \in \mathbb{E}$ is such that θ, η and $\theta\eta$ are pure quaternions. Let $p \in \mathbb{Z}$ be a prime such that p divides $\mathrm{N}(\theta)$ and $\mathrm{N}(\eta)$. Then $p \mid \theta\eta$.*

Proof. Suppose that p does not divide $\theta\eta$. By Lemma 2.5 and Lemma 4.1, we have $\theta = \pi_1\theta_1$, $\eta = \eta_1\pi_2$, and $\theta\eta = \pi\delta_1\overline{\pi}$, where π, π_1, π_2 have norm p. By the uniqueness part of Lemma 2.5, π, π_1, and $\overline{\pi_2}$ are right associates; however, θ, η, and $\theta\eta$ are pure quaternions, so $\theta\eta = -\overline{\theta\eta} = -\overline{\eta}\,\overline{\theta} = -\eta\theta = -\eta_1\pi_2\pi_1\theta_1$ is divisible by p, a contradiction. □

Lemma 5.6. *Suppose $\theta, \eta \in \mathbb{E}$ is such that θ, η, and $\theta\eta$ are pure quaternions. Let $p \in \mathbb{Z}$ be a prime such that p^2 divides both $\mathrm{N}(\theta)$ and $\mathrm{N}(\eta)$, but p does not divide both θ and η. Then there exist elements $\pi, \theta_1, \eta_1 \in \mathbb{E}$ such that $\mathrm{N}(\pi) = p$, $\theta = \pi\theta_1\overline{\pi}$, and $\eta = \pi\eta_1\overline{\pi}$.*

Proof. By Lemma 5.5, $p \mid \delta = \theta\eta$. Using Lemma 4.1, we can write $\theta = \pi\theta_1\overline{\pi}$ and $\eta = \pi_1\eta_1\overline{\pi_1}$, where $\mathrm{N}(\pi) = \mathrm{N}(\pi_1) = p$. Since θ is pure, $\delta = \theta\eta = -\overline{\theta}\eta$, and Lemma 2.6 shows that $\pi \mid \eta$. Applying the uniqueness part of Lemma 2.5 to η, we obtain that π and π_1 are right associates. □

Lemma 5.7. *Suppose $\theta, \eta \in \mathbb{E}$ is such that θ, η, and $\theta\eta$ are pure quaternions. Let $p \in \mathbb{Z}$ be a prime such that p^2 divides $\mathrm{N}(\theta)$ but p does not divide θ. Then there exist elements $\pi, \theta_1, \eta_1 \in \mathbb{E}$ such that $\mathrm{N}(\pi) = p$, $\theta = \pi\theta_1\overline{\pi}$, and $p\eta = \pi\eta_1\overline{\pi}$.*

Proof. Again, write $\theta = \pi\theta_1\overline{\pi}$. Suppose first that $\pi \mid \eta$, that is, $\eta = \pi\eta_2$, for some $\eta_2 \in \mathbb{E}$. Then $p\eta = \pi(\eta_2\pi)\overline{\pi}$, and we are done in this case. So, we can assume that π does not divide η. Since θ is pure, $\delta = \theta\eta = -\overline{\theta}\eta$, and Lemma 2.6 shows that p does not divide δ. By Lemma 4.1 and the uniqueness part of Lemma 2.5, we have $\delta = \pi\delta_1\overline{\pi}$. Then $\pi\theta_1\overline{\pi}\eta = \delta = \pi\delta_1\overline{\pi}$ implies that $\theta_1\overline{\pi}\eta\pi = \delta_1\overline{\pi}\pi = p\delta_1$. Hence, $p \mid \overline{\overline{\pi}\eta\pi}\,\theta_1$. Lemma 2.6 shows that either $\overline{\pi} \mid \theta_1$ or $p \mid \overline{\pi}\eta\pi$. The first case is impossible because then θ would be divisible by p. If we let $\overline{\pi}\eta\pi = p\eta_1$, then $p\eta = \pi\eta_1\overline{\pi}$. □

Proposition 5.8. *Every pair (θ, η) of twins is parameterized by a pair $(\alpha, z) \in \mathbb{E} \times \mathbb{G}$.*

Proof. Let $M = \mathrm{N}(\theta) = \mathrm{N}(\eta)$. Consider all representations of the form $\theta = \alpha\theta_1\overline{\alpha}$ and $\eta = \alpha\eta_1\overline{\alpha}$, where $\alpha, \theta_1, \eta_1 \in \mathbb{E}$. Clearly, θ_1 and η_1 are twins as well. There exists such a representation (with $\alpha = 1$), and so there is one with $\mathrm{N}(\alpha)$ as large as possible. We present reductions to increase $\mathrm{N}(\alpha)$.

If p is a prime such that p^2 divides both $\mathrm{N}(\theta_1)$ and $\mathrm{N}(\eta_1)$, but p divides neither θ_1 nor η_1, then Lemma 5.6 allows us to replace α with $\alpha\pi$. If this p does not divide θ_1 but divides η_1, then we write $\eta_1 = p^\ell\eta'$ such that η' is not divisible by p, and apply Lemma 5.7 to θ_1 and η'. We again obtain a suitable π by using up a factor of p out of p^ℓ.

If none of these reductions can be performed further, then $\theta_1 = d\theta_2$ and $\eta_1 = d\eta_2$, for some $d \in \mathbb{Z}$ such that $\mathrm{N}(\theta_2) = \mathrm{N}(\eta_2)$ is square-free. By Lemma 5.5, every integer prime divisor of $\mathrm{N}(\eta_2)$ divides $\theta_2\eta_2$. Hence, the square-free integer $\mathrm{N}(\eta_2)$ divides $\theta_2\eta_2$, whose norm is $\mathrm{N}(\eta_2)^2$. Therefore, $\theta_2\eta_2 = \mathrm{N}(\eta_2)\varepsilon$, where ε is a unit of $\mathbb{E}$. We may assume $\varepsilon = i$, by the argument in the last paragraph of the proof of Theorem 4.2. Thus, $\eta_2 = \theta_2 i$, and as θ_2 and η_2 are pure quaternions, $\theta_2 = z_1 j$, for some $z_1 \in \mathbb{G}$. Then $\theta = \alpha(dz_1)j\,\overline{\alpha}$ and $\eta = \alpha(dz_1)k\,\overline{\alpha}$, proving the claim. □

Lemma 5.9. *Let $(\alpha, z) \in \mathbb{H} \times \mathbb{C}$ and suppose that $z = s^2 t$, for some $s, t \in \mathbb{C}$. Then the pairs (α, z) and $(\alpha s, t)$ are equivalent.*

Proof. Since $jsj^{-1} = \overline{s}$ for every $s \in \mathbb{C}$, we have that $zj = stj\,\overline{s}$ and similarly, $zk = stk\,\overline{s}$. Therefore, $\alpha zj\,\overline{\alpha} = (\alpha s)tj(\overline{\alpha s})$ and $\alpha zk\,\overline{\alpha} = (\alpha s)tk(\overline{\alpha s})$. □

This lemma immediately implies (2) of Theorem 5.4 ((1) has been proven in Proposition 5.8). We now proceed to prove (3). If a suitable ρ in (3) exists, then (α_1, z_1) is

equivalent to $(\alpha_1\rho, z_2) = (\alpha_2, z_2)$, by Lemma 5.9. We now only have to prove that if (α_1, z_1) and (α_2, z_2) are equivalent pairs in $\mathbb{E} \times \mathbb{G}$, then a suitable ρ exists.

Choose elements $s_r \in \mathbb{C}$ satisfying $s_r^2 = z_r$. Lemma 5.9 shows that (α_r, z_r) is equivalent to $(\alpha_r s_r, 1)$. From $(\alpha_1 s_1)j(\overline{\alpha_1 s_1}) = (\alpha_2 s_2)j(\overline{\alpha_2 s_2})$, we get that $(\alpha_2 s_2)^{-1}(\alpha_1 s_1)$ centralizes j (as well as k, by the same calculation). Since the elements of $\mathbb{H}$ centralizing both j and k are exactly the real numbers, we get that $t = (\alpha_2 s_2)^{-1}(\alpha_1 s_1)$ is contained in $\mathbb{R}$. This can be written as $t\alpha_1^{-1}\alpha_2 = s_1 s_2^{-1}$. From $(\alpha_1 s_1)j(\overline{\alpha_1 s_1}) = (\alpha_2 s_2)j(\overline{\alpha_2 s_2})$, we get that $\mathrm{N}(\alpha_1)^2\,\mathrm{N}(s_1)^2 = \mathrm{N}(\alpha_2)^2\,\mathrm{N}(s_2)^2$. Hence $\mathrm{N}(t) = 1$, and $t = \pm 1$.

This implies that $\alpha_1^{-1}\alpha_2 = \rho$ is a complex number with rational components, and $\rho^2 = (s_1 s_2^{-1})^2 = z_1 z_2^{-1}$. Therefore, $z_1 z_2 = (\rho z_2)^2$. The ring of Gaussian integers is integrally closed in the field of Gaussian numbers, so $\rho z_2 \in \mathbb{G}$. Since z_1 and z_2 are square-free, each Gaussian prime divisor of z_1 has multiplicity 1 in both z_1 and z_2, with the same holding for z_2. We see that z_1 and z_2 are associates, and ρ^2 is a unit in $\mathbb{G}$. Thus, ρ is a unit in $\mathbb{G}$, establishing (3) of Theorem 5.4.

Finally, we prove (4). Suppose that (α, z) parameterizes the twin pair (θ, η). Then $\mathrm{N}(\theta) = \mathrm{N}(\alpha)^2\,\mathrm{N}(z)$ is a square if and only if $\mathrm{N}(z)$ is a square. Clearly, if $z \in \mathbb{Z}$ or $iz \in \mathbb{Z}$, then $\mathrm{N}(z)$ is a square.

Suppose that $\mathrm{N}(z)$ is a square and consider a Gaussian prime divisor π of z. As z is square-free in $\mathbb{G}$, the number π^2 does not divide z. We show that $\pi = 1 + i$ is impossible. Indeed, all other Gaussian primes have odd norm, so $\mathrm{N}(z)$ would have to be of the form $4k+2$, which cannot be the square of an integer. Similarly, if $p = \mathrm{N}(\pi)$ is an odd prime (of the from $4k + 1$), then $p \mid \mathrm{N}(z)$, and so the conjugate of π must also be a factor of z. Therefore, z is indeed either real or pure imaginary, and the proof of Theorem 5.4 is complete. □

Theorem 5.10. *For a positive integer M, denote by $\mathrm{T}(M)$ the number of twin pairs (θ, η) such that $\mathrm{N}(\theta) = \mathrm{N}(\eta) = M$, and let $\sigma(s)$ be the sum of positive integer divisors of any integer s. Suppose that*

$$M = 2^\kappa p_1^{\lambda_1} \dots p_m^{\lambda_m} q_1^{\mu_1} \dots q_\ell^{\mu_\ell}\,,$$

where $p_1, \dots, p_m$ are primes $\equiv 1\ (4)$ and $q_1, \dots, q_\ell$ are primes $\equiv -1\ (4)$. We assume that all λ_r and μ_s are positive. Then

$$\mathrm{T}(M) = 24 \prod_{r=1}^{m} g(p_r^{\lambda_r}) \prod_{s=1}^{\ell} h(q_s^{\mu_s})\,,$$

where

$$g(p^{2\lambda}) = \sigma(p^\lambda) + \sigma(p^{\lambda-1})\,, \qquad g(p^{2\lambda+1}) = 2\sigma(p^\lambda)\,,$$

and

$$h(q^{2\mu}) = \sigma(q^\mu) + \sigma(q^{\mu-1})\,, \qquad h(q^{2\mu+1}) = 0\,.$$

In particular, $\mathrm{T}(M)/24$ is a multiplicative function. If there exists a twin pair with norm M, then M is the sum of two squares.

Proof. By Theorem 5.4, we have to count the number of pairs $(\alpha, z) \in \mathbb{E} \times \mathbb{G}$, where $M = \mathrm{N}(\alpha)^2 \, \mathrm{N}(z)$ and z is square-free in $\mathbb{G}$, and divide the number of solutions by 4 due to (3).

Writing z as a product of Gaussian primes, we see that in the canonical form of $\mathrm{N}(z)$ every prime of the form $4k+3$ has exponent 2, every prime of the form $4k+1$ has exponent 2 or 1, and the prime 2 has exponent 1 (or 0). If such a number $t = \mathrm{N}(z)$ is given, then the only freedom in determining z occurs at the primes p of the form $4k+1$. Indeed, $p = \pi_1 \overline{\pi_1}$ is a product of two Gaussian primes, and if the exponent of p in $\mathrm{N}(z)$ is 1, then we can decide whether to put π or $\overline{\pi}$ into z. We have to multiply the resulting z with the four Gaussian units. Thus, if $4f(t)$ denotes the number of solutions for z with norm t, then f is a multiplicative function, which is 1 or 0 for every prime power, except that $f(p^1) = 2$ when $p \equiv 1 \ (4)$.

Corollary 2.8 allows us to count the number of integral quaternions α with given norm $\mathrm{N}(\alpha)$. The result is 24 times a multiplicative function (the sum of odd divisors of $\mathrm{N}(\alpha)$). We now go through all primes in the decomposition of M to see how we can split M into $\mathrm{N}(\alpha)^2 \, \mathrm{N}(z)$.

If the prime is 2, then we must put 2^κ into $\mathrm{N}(\alpha)^2$ when κ is even, and must put $2^{\kappa-1}$ into $\mathrm{N}(\alpha)^2$ when κ is odd. By Corollary 2.8, we see that $\mathrm{T}(2^\kappa) = 24$, and $\mathrm{T}(M)$ does not depend on κ.

Next, we consider a prime $q_r \equiv -1 \ (4)$. In this case, μ_r must be even for a solution to exist, and we can either put the entire $q_r^{\mu_r}$ into $\mathrm{N}(\alpha)^2$ or put $q_r^{\mu_r - 2}$ into $\mathrm{N}(\alpha)^2$ and q_r into z. This proves the formula in the theorem for h.

Finally, for $p_r \equiv 1 \ (4)$ there are two cases to consider. If λ_r is even, then we can put 0 or 2 copies of p_r into $\mathrm{N}(z)$. If λ_r is odd, then we must put 1 copy of p_r into $\mathrm{N}(z)$ (and the corresponding Gaussian primes in z can be chosen in 2 ways). This proves the formula for g.

Since we can put together the solutions for M from the solutions for the prime divisors of M independently, we get the formula in the theorem. □

Corollary 5.11. *Let (v, w) be a pair of twins in $\mathbb{Z}^3$ whose length is an integer. Then there exists an $\alpha \in \mathbb{E}$ and an integer d such that the last two columns of $dE(\alpha)$ are either (v, w) or $(-w, v)$. Therefore, (v, w) can be extended to an icube.*

Proof. Let $\big(V(v), V(w)\big) = (\theta, \eta)$ be parameterized by (α, z), where z is square-free. By (4) of Theorem 5.4, z is either real or pure imaginary, so $z = d$ or $z = di$ for some integer d. In the first case, $\theta = d\alpha j \, \overline{\alpha}$ and $\eta = d\alpha k \, \overline{\alpha}$, so the last two columns of $dE(\alpha)$ are v and w. In the second case, $\theta = d\alpha k \, \overline{\alpha}$ and $\eta = -d\alpha j \, \overline{\alpha}$, so the last two columns of $dE(\alpha)$ are $-w$ and v. □

Corollary 5.12. *If (u, v, w) is an icube, then there is an $\alpha \in \mathbb{E}$ and $d \in \mathbb{Z}$ such that (u, v, w) and $dE(\alpha)$ can be obtained from each other by permuting and changing the signs of certain columns.*

Proof. By Proposition 1.3, the edge length is an integer. Let α and d be given by Corollary 5.11. Then the columns of $dE(\alpha)$ and $(\pm u, \pm v, \pm w)$ share two orthogonal vectors, and so they share the third column of $E(\alpha)$ as well. □

Lemma 5.13. *Suppose that $\alpha \in \mathbb{E}$, z is a square-free Gaussian integer and $\theta = \alpha z j \overline{\alpha}$ is primitive. Then $\mathrm{N}(z)$ is the square-free part of $\mathrm{N}(\theta)$.*

Proof. As $\mathrm{N}(\theta) = \mathrm{N}(\alpha)^2 \mathrm{N}(z)$, it is sufficient to prove that $\mathrm{N}(z)$ is square-free. Suppose that $p^2 \mid \mathrm{N}(z)$, for a prime $0 < p \in \mathbb{Z}$. If $p \equiv 3\ (4)$, then p is a Gaussian prime, so $p \mid z$, contradicting the fact that θ is primitive. If $p = 2$, then $2 \mid z$, a contradiction. Finally, if $p = \pi\overline{\pi}$, for some Gaussian prime π, then π and $\overline{\pi}$ cannot both divide z, because then p would divide the primitive θ. On the other hand, the exponent of π and $\overline{\pi}$ is at most 1 in z, since z is square-free. Therefore, $\mathrm{N}(z)$ cannot be divisible by p^2, a contradiction. □

Proof of Theorem 1.5. We have proved the existence statement in Remark 4.3. Suppose that x is primitive. If (u, v, w) is an icube with edge length m such that $x = au + bv + cw$, then (u, v, w) is also primitive. Therefore, by Corollary 5.12 (or by Corollary 3.9), we may assume that $(u, v, w) = E(\alpha)$, for some $\alpha \in \mathbb{E}$. Thus, it is sufficient to deal with "Eulerian" cubic lattices.

Suppose that x is contained in two such sublattices: $V(x) = \alpha_1\beta_1\,\overline{\alpha_1} = \alpha_2\beta_2\,\overline{\alpha_2}$. By the uniqueness part of Theorem 4.2, there exists a unit $\varepsilon \in \mathbb{E}$ such that $\alpha_2 = \alpha_1\varepsilon^{-1}$, and β_2, β_1 are group-conjugates via ε. Propositions 3.1 and 3.2 show that the matrices $E(\alpha_1)$ and $E(\alpha_2)$ may differ only by permutations and sign changes of columns. Therefore, the two cubic lattices are actually the same, proving the uniqueness part of the theorem. □

Proof of Corollary 1.6. Using the notation of the previous proof, let L denote the unique sublattice obtained there. Proposition 3.2 shows that β_1 and β_2 have the same number of zero components. Therefore, when considering the three cases of Corollary 1.6 (which are distinguished by the number of zero components of x relative to L), it does not matter which generating α we choose for L.

We now show that every twin of x is contained in L. Let η_1 be a twin of $\theta = V(x)$, and let (α_1, z_1) parameterize the pair (θ, η_1), with z_1 square-free. By Lemma 5.13, $\mathrm{N}(z_1) = n$, and so $\mathrm{N}(\alpha_1) = m$. Thus, the sublattice generated by α_1 is L. Since $z_1 j$ has a zero component, by case (1) of Corollary 1.6, the vector x cannot have a twin.

If the norm of x is a square, then $1 = n = \mathrm{N}(z_1)$, and $z_1 \in \{\pm 1, \pm i\}$. Thus, x and each of its twins has exactly one nonzero component relative to L. Therefore, x has exactly 4 twins. Conversely, if x has only one nonzero component relative to L, then its length is obviously an integer, since the same holds for the generating vectors of L. Hence, (3) is proved.

Finally, suppose that none of the components of z_1 is zero (so x has exactly one zero component). Let η_2 be another twin of θ, parameterized by (α_2, z_2). Again,

$\alpha_2 = \alpha_1\varepsilon^{-1}$ and $\varepsilon z_1 j\varepsilon^{-1} = z_2 j$, for some unit ε; however, not every unit ε yields a twin of θ. Indeed, if $\varepsilon \notin Q = \{\pm 1, \pm i, \pm j, \pm k\}$, then Proposition 3.2 shows that group-conjugation by ε induces a fixed point free permutation on the components of the vectors (while possibly changing some signs). We know that the first component of $z_1 j$ and of $z_2 j$ is zero. Therefore, $\varepsilon \notin Q$ can happen only if $z_1 j$ and $z_2 j$ have two nonzero components, which we have excluded. Thus, $\varepsilon \in Q$. The two twins of θ in question are $\eta_1 = \alpha_1 z_1 k\,\overline{\alpha_1}$ and

$$\eta_2 = \alpha_2 z_2 k\,\overline{\alpha_2} = -\alpha_1 z_1 (j\varepsilon^{-1} i \varepsilon)\overline{\alpha_1}\,.$$

Let us calculate this now.

If $\varepsilon \in \{\pm 1, \pm i\}$, then $\eta_2 = \eta_1$. (This has been noted in (3) of Theorem 5.4.)

If $\varepsilon \in \{\pm j, \pm k\}$, then $\eta_2 = -\eta_1$ (This is always obviously another twin of θ.)

Thus, if x has two nonzero components relative to L, then it has no more than two twins, completing the proof of Corollary 1.6. □

6. Twin-complete numbers

In this section we first prove the characterization of twin-complete numbers given in Theorem 1.8 and then discuss Conjecture 1.9.

Lemma 6.1. *If $4n$ is twin-complete, then so is n.*

Proof. Every pure quaternion whose norm is divisible by 4 is divisible by 2. This follows by looking at the coefficients mod 4 (or from Theorem 4.6). Thus, if $\mathrm{N}(\theta) = n$, then 2θ has a twin η, and so $\eta/2$ is a twin of θ. □

Lemma 6.2. *Let $\beta \in \mathbb{E}$ be a primitive pure quaternion and $m > 0$ an odd positive integer. Then there exists an $\alpha \in \mathbb{E}$ with norm m such that $\alpha\beta\,\overline{\alpha}$ is primitive.*

Proof. It is sufficient to prove this when m is a prime, since we can go through the prime divisors of m one by one. Clearly (or by Theorem 4.6), $\alpha\beta\,\overline{\alpha}$ is primitive if and only if it is not divisible by $p = m$. By Proposition 4.7, there is such an α (we have actually counted them). □

Proof of Theorem 1.8. Let $n, m > 0$ be integers, with n square-free. Suppose that n is twin-complete. It is sufficient to prove that every primitive vector δ with norm nm^2 has a twin (since we can do induction on m). By Theorem 4.2, $\delta = \alpha\beta\,\overline{\alpha}$, for some $\alpha, \beta \in \mathbb{E}$ such that $\mathrm{N}(\alpha) = m$ and $\mathrm{N}(\beta) = n$. Since n is twin-complete, β has a twin γ. We show that $\alpha\gamma\,\overline{\alpha}$ is a twin of δ, using Proposition 5.1. Indeed,

$$\delta\alpha\gamma\,\overline{\alpha} = \alpha\beta(\overline{\alpha}\alpha)\gamma\,\overline{\alpha} = m\alpha\beta\gamma\overline{\alpha}\,.$$

This is a pure quaternion, since $\beta\gamma$ is a pure quaternion. This proves one direction of the theorem.

For the converse, suppose that $n > 0$ is square-free and nm^2 is twin-complete. Then every vector β with norm n is primitive. By Lemma 6.1, we may assume that

m is odd. For any given β, Lemma 6.2 yields an α with norm m such that $\theta = \alpha\beta\,\overline{\alpha}$ is primitive. Since nm^2 is twin-complete, θ has a twin. By Theorem 5.4, this pair of twins can be parameterized by some $(\alpha_1, z) \in \mathbb{E} \times \mathbb{G}$ such that z is square-free. Thus, $\theta = \alpha_1 z j\,\overline{\alpha_1}$, and by Lemma 5.13, $\mathrm{N}(z)$ is the square-free part of $\mathrm{N}(\theta)$, that is, $\mathrm{N}(z) = n$ and $\mathrm{N}(\alpha_1) = m$. By the uniqueness statement of Theorem 4.2, we get that $\beta = \varepsilon z j \varepsilon^{-1}$, for some unit $\varepsilon \in \mathbb{E}$, but then $\varepsilon z k \varepsilon^{-1}$ is a twin of β. Hence, n is twin-complete.

To prove the last statement of the theorem, let n be square-free. Clearly, $(a, b, 0)$ and $(-b, a, 0)$ are twins, so if n is not the sum of three positive squares, but is the sum of two squares, then it is twin-complete. Conversely, suppose that n is twin-complete. Let β be a pure quaternion of norm n, we have to show that at least one of the three coordinates of the corresponding vector is zero. As n is twin-complete, β has a twin, so Theorem 5.4 implies that $\beta = \alpha z j\,\overline{\alpha}$, for some $(\alpha, z) \in \mathbb{E} \times \mathbb{G}$. Here $n = \mathrm{N}(\beta) = \mathrm{N}(\alpha)^2\,\mathrm{N}(z)$, so $\mathrm{N}(\alpha) = 1$ and α is a unit. From Proposition 3.2, we get that at least one component of β is zero (since this is the case with zj). □

Now we discuss Conjecture 1.9. Let

$$S \supseteq \{1, 2, 5, 10, 13, 37, 58, 85, 130\}$$

denote the list of those square-free numbers that can be written as a sum of two squares, but not as a sum of three positive squares. It has been known since [GCC59] that this list is finite, and if the conjecture fails, there is at most one number in S not listed above ([Wei73], [Gro85]).

In [Mor60], it is shown that for an integer $n \in S$, the only nonnegative solutions of

$$xy + yz + zx = n$$

when $n \equiv 2\ (4)$ are given by $xyz = 0$, and when $n \equiv 1\ (4)$ are given by either $xyz = 0$ or $x = d$, $y = d$, $z = (n - d^2)/2d$, where d is any divisor of n with $d^2 < n$. Either way, for such numbers n the above equation has no solution with three distinct positive integers x, y, z.

This characterization of the numbers in S allows us to see the relationship they bear with Euler's *numeri idonei*. Euler defined a *numerus idoneus* to be an integer N such that, for any positive integer m, if

$$m = x^2 \pm Ny^2, \quad (x^2, Ny^2) = 1, \quad x, y \geq 0$$

has a unique solution, then m is of the form $2^a p^k$, $a \in \{0, 1\}$, $k \geq 1$, p is a prime.

Euler was aware of 65 *numeri idonei*, and it is widely believed and conjectured that this list is complete ([Rib00]). S. Chowla proved in [Cho34] that there are only finitely many *numeri idonei*, and P. J. Weinberger improved this result by showing that there can be at most one more square-free idoneal number, and, if it exists, it must be greater than $2 \cdot 10^{11}$ ([Wei73]). If there is indeed another square-free idoneal number N, and it is even, then $4N$ is also idoneal. On the other hand, if $N > 1848$

is idoneal and not square-free, then $N/4$ is both square-free and idoneal ([Kan09]). Thus, there are at most 67 idoneal numbers.

Using Theorem 3.22 of [Cox89] it can be shown that an integer N is a *numerus idoneus* if and only if it cannot be expressed as $xy + yz + zx$ with $0 < x < y < z$. Combining this with the characterization by [Mor60] described above, we see that every integer in S is also one of Euler's *numeri idonei*. Checking Euler's list of the 65 *numeri idonei* (the greatest of which is only 1848) against the properties listed in Conjecture 1.9, one sees that, indeed, Conjecture 1.9 is true if Euler's list is complete.

If we only consider those integers n for which there is no representation of the form $xy + yz + zx$ with $1 \leq x \leq y \leq z$, i.e., the even, square-free, twin-complete numbers, then we have from [BC00] that such an n can only be absent from the list of Conjecture 1.9 if the Generalized Riemann Hypothesis fails.

References

[BC00] J. Borwein, K. K. S. Choi, *On the representations of $xy + yz + zx$*, Exp. Math. **9** (2000), 153–158.

[Car15] R. D. Carmichael, *Diophantine analysis*, John Wiley & Sons, 1915.

[Cho34] S. Chowla, *An extension of Heilbronn's class number theorem*, Quart. J. Math. Oxford **5** (1934), 304–307.

[CS03] J. H. Conway, D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic and Symmetry*, A K Peters, 2003.

[Cox89] D. A. Cox, *Primes of the form $x^2 + ny^2$*, New York: John Wiley & Sons, 1989.

[GCC59] E. Grosswald, A. Calloway, J. Calloway, *The representation of integers by three positive squares*, Proc. Amer. Math. Soc. **10** (1959), 451–455.

[Gro85] E. Grosswald, *Representations of integers as sums of squares*, New York: Springer-Verlag, 1985.

[HW79] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers, 5th Ed.*, Oxford: Clarendon Press, 1979.

[H19] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, 1919.

[Kan09] E. Kani, *Idoneal numbers and some generalizations*, preprint (2009), available at `http://www.mast.queensu.ca/~kani/papers/idoneal.pdf`

[Mor60] L. J. Mordell, *The representation of integers by three positive squares*, Mich. Math. J. **7** (1960), 289–290.

[Pal40] G. Pall, *On the arithmetic of quaternions*, Tran. Amer. Math. Soc. **47** (1940), 487–500.

[Rib00] P. Ribenboim, *My numbers, my friends.* Popular Lectures on Number Theory. Springer-Verlag, Berlin-Heidelberg, 2000.

[Sar61] A. Sárközy, *On lattice-cubes in the three-space* (in Hungarian), Matematikai Lapok, 1961.

[Wei73] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124.

(Lee M. Goswick) The University of Alabama at Birmingham, Department of Mathematics, 1300 University Blvd., Suite 452, Birmingham, AL 35294 U.S.A.

(Emil W. Kiss) Eötvös University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary

(Gábor Moussong) Eötvös University, Department of Geometry, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary

(Nándor Simányi) The University of Alabama at Birmingham, Department of Mathematics, 1300 University Blvd., Suite 452, Birmingham, AL 35294 U.S.A.

E-mail address, Lee M. Goswick: goswick@amadeus.math.uab.edu

E-mail address, Emil W. Kiss: ewkiss@math.elte.hu

E-mail address, Gábor Moussong: mg@math.elte.hu

E-mail address, Nándor Simányi: simanyi@math.uab.edu