

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 characterized modulo a famous conjecture in number theory. The main tool is the decomposition theory of Hurwitz integral quaternions, but elementary, geometric proofs are provided for most of the results as well.

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 $\|v_i\|^2$ (a similar convention is used also for Gaussian integers and quaternions). Thus the norm of an integral vector is an integer, but the length is not necessarily.

In this paper we investigate how icubes can be *constructed*, *counted*, and *extended*. We mainly consider the case $n = 3$ and $k = 2$, but shall make some easy observations concerning higher dimensional icubes as well, and formulate the corresponding problems in Section 9.

Before listing the motivating problems and the results in more detail, let us make a remark about our methods. Many theorems will be obtained either by elementary calculations (Sections 3, 8) or by geometrical arguments (Section 7). On the other hand, all the results in the paper can be proved using the number theory of Hurwitz integral quaternions (see Section 2 for definitions concerning quaternions). These arguments occupy Sections 4, 5 and 6. We made an effort to keep these sections “clean” in the sense that we do not refer here to the proofs in the other sections.

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.

Except for some side remarks, we never use the deeper methods of number theory, like quadratic extensions, modular forms, analytic tools. However, we believe that analytic methods will be useful in dealing with the problems in Section 9.

Proposition 1.1. *Let (v_1, \dots, 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, \dots, v_n) . But d^2 is also an integer, since the vectors have integer components. Hence d^{n-1} is an integer, too. Therefore $d = d^n/d^{n-1}$ is rational, and so it is an integer. \square

Three dimensional icubes in \mathbb{Z}^3 have been described by A. Sárközy [Sar61]. To formulate his main result, we go back to a construction discovered by Euler. The following well-known facts show how to obtain rotations in \mathbb{R}^3 . A *rotation* is an orientation-preserving orthogonal map, that is, an element of the group $\text{SO}(3)$. Throughout the paper we identify $v = (v_1, v_2, v_3) \in \mathbb{R}^3$ with the pure quaternion $V(v) = v_1i + v_2j + v_3k$.

Theorem 1.2. *For a quaternion α define the map $R(\alpha) : \beta \mapsto \alpha\beta\bar{\alpha}$ on the set of pure quaternions β . Then $\alpha\beta\bar{\alpha}$ is also a pure quaternion, so $R(\alpha)$ can be considered as a map $\mathbb{R}^3 \rightarrow \mathbb{R}^3$.*

- (1) *If the norm of α is 1 (that is, if α is a unit quaternion), then $R(\alpha)$ is a rotation. (In this case $R(\alpha)$ is conjugation by α in the sense of group theory).*
- (2) *Every rotation is of the form $R(\alpha)$, and this α is unique up to sign.*
- (3) *Let $\alpha = m + ni + pj + qk$ whose norm is $d = |\alpha|^2 = m^2 + n^2 + p^2 + q^2$. Then $R(\alpha)$ is a dilated rotation, where the dilation coefficient is d . The matrix of $R(\alpha)$ in the standard basis (i, j, k) is denoted by $E(\alpha)$. It is the Euler matrix*

$$E(\alpha) = \begin{pmatrix} m^2 + n^2 - p^2 - q^2 & -2mq + 2np & 2mp + 2nq \\ 2mq + 2np & m^2 - n^2 + p^2 - q^2 & -2mn + 2pq \\ -2mp + 2nq & 2mn + 2pq & m^2 - n^2 - p^2 + q^2 \end{pmatrix}.$$

Thus the columns of the Euler matrix are pairwise orthogonal, and have common length d . We are interested in this matrix 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 1.3 (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 icubes with a given edge length d . His proof uses Jacobi's classical result on the number of decompositions of integers to the sum of four squares (Theorem 2.15).

Now we turn our attention to the question of *extension*. The above result makes it easy to answer the following question: 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 1.1 is sufficient.

Theorem 1.4. *A vector in \mathbb{Z}^3 is contained in an icube iff 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 1915 (see [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) . Thus (gu, gv, gw) extends $x = gu$. \square

Here we referred to the *Euler parameterization of Pythagorean quadruples*. Theorem 8.1 gives the detailed statement with a constructive proof. Theorem 4.2 also yields Theorem 1.4 using quaternions (see Remark 4.3). A geometrical proof is given in Theorem 7.4 and Corollary 7.5. When u is primitive, the cubic lattice generated by any 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 (Corollary 5.11), and there is an elementary proof (Proposition 7.1).

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

Theorem 1.5. *Let $x \in \mathbb{Z}^3$ have norm nm^2 , where n is squarefree. 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. See Corollary 7.5 for an elementary argument in the case when x has integer length.

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 says 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. However, 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 tells us 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 question of extension is more difficult to handle. A consequence of this counting result is that the common norm of twins is always the sum of two squares (Proposition 7.6 gives an elementary proof). However, the converse 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 described as follows (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 is 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. A positive integer M is called *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 iff its squarefree part is twin-complete. A positive squarefree integer is twin-complete if and only if it can be written as a sum of at most two positive 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 squarefree numbers that can be written as a sum of at most two positive 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. \square*

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

2. INTEGRAL QUATERNIONS

In this section we list some basic results about the number theory of the ring of \mathbb{G} of Gaussian integers, and of the ring \mathbb{E} of Hurwitz integral quaternions. We assume that the reader is familiar with the fact that \mathbb{G} has unique factorization, and with the description of Gauss primes. We shall need the following observation.

Lemma 2.1. *If α is complex number with rational real and imaginary part and $\alpha^2 \in \mathbb{G}$, then $\alpha \in \mathbb{G}$.*

Proof. Write $\alpha = \beta/d$, where $\beta \in \mathbb{G}$ and $d \in \mathbb{Z}$. Then $d^2 \mid \beta^2$ among Gaussian integers, hence $d \mid \beta$, so $\alpha = \beta/d \in \mathbb{G}$. Here we used unique factorization in \mathbb{G} . \square

Next we review the well-known theorems about decompositions to sums of squares.

Theorem 2.2 (Fermat). *A positive integer d is the sum of two (integer) squares if and only if in the prime factorization of d every prime of the form $4k - 1$ occurs an even number of times. The number of decompositions is $4 \prod (\mu_j + 1)$, where the μ_j are the exponents of the primes of the form $4k + 1$ in the canonical form of d .*

This can be proved easily using Gaussian integers.

Theorem 2.3 (Lagrange). *A positive integer d is not the sum of three squares if and only if d is of the form $4^n(8k + 7)$ with some non-negative integers n and k .*

Here it is harder to find the number of decompositions, but the problem can be reduced to the case when d is squarefree. The corresponding formula is given by (29) in [Pal40]. We include it as Corollary 4.9, because it falls out from the results in Section 4.

Theorem 2.4 (Lagrange). *Every positive integer is the sum of four squares.*

There is an explicit formula for the number of solutions. We shall state it in Theorem 2.15, because it is related to the number of irreducible quaternions.

Now we look at the number theory of integral quaternions. The general reference is [H19]. The division ring of all quaternions (with real coefficients) is denoted by \mathbb{H} .

Definition 2.5. Let $\alpha = a + bi + cj + dk \in \mathbb{H}$ be a quaternion ($a, b, c, d \in \mathbb{R}$). Then

$$\bar{\alpha} = a - bi - cj - dk$$

is the *conjugate* of α ,

$$N(\alpha) = a^2 + b^2 + c^2 + d^2 = \alpha\bar{\alpha} = \bar{\alpha}\alpha$$

is the *norm* of α , and

$$\text{tr}(\alpha) = 2a = \alpha + \bar{\alpha}$$

is the *trace* of α . Therefore

$$\alpha^2 - \text{tr}(\alpha)\alpha + N(\alpha) = 0.$$

A quaternion is *pure* if its trace is zero. We define the special element

$$\sigma = \frac{1 + i + j + k}{2}.$$

Proposition 2.6 ([HW79]). *We have $\overline{\alpha\beta} = \overline{\beta} \overline{\alpha}$ and $N(\alpha\beta) = N(\alpha)N(\beta)$ for every $\alpha, \beta \in \mathbb{H}$. We have $N(\sigma) = 1$ and $\sigma^2 = \sigma - 1$. Conjugating by σ induces a cyclic permutation on $\{i, j, k\}$ (see Section 3 for more details).*

Definition 2.7. Quaternions of the form

$$a\sigma + bi + cj + dk \quad (a, b, c, d \in \mathbb{Z})$$

are called *integral quaternions*, or *Hurwitz integral quaternions*; they form a ring \mathbb{E} . Quaternions of the form

$$a + bi + cj + dk \quad (a, b, c, d \in \mathbb{Z})$$

shall be called *quaternions with integer coefficients*, or *Lipschitz integral quaternions*. Such a quaternion is called *primitive* if $\gcd(a, b, c, d) = 1$.

Proposition 2.8. *A quaternion $\alpha = a + bi + cj + dk$ is Hurwitz if and only if either a, b, c, d are all integers, or all of them is the half of an odd integer. If α is such, then $N(\alpha)$, $\text{tr}(\alpha)$ are integers. 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.*

We shall be working exclusively in the ring \mathbb{E} of Hurwitz integral quaternions, and use the divisibility symbol $|$ to denote divisibility *on the left* in \mathbb{E} . The rings \mathbb{Z} and \mathbb{G} are subrings of \mathbb{E} , and it is easy to see that here $|$ retains its usual meaning.

Proposition 2.9. *An integral quaternion is a unit (that is, divides every element of \mathbb{E} on the left) if and only if its norm is 1. These are exactly the 24 elements*

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \frac{\pm 1 \pm i \pm j \pm k}{2},$$

which form a group under multiplication. Every integral quaternion has a left associate that has integer coefficients ([HW79], p. 305).

Theorem 2.10. *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 $N(\rho) < N(\beta)$ (see Theorem 373 of [HW79]).*

The ring \mathbb{E} is also left Euclidean. In fact, $\alpha \mapsto \overline{\alpha}$ is an isomorphism between \mathbb{E} and its dual, so every assertion that we prove for \mathbb{E} holds also 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. For us, it will be sufficient to use the following two lemmas for uniqueness.

Lemma 2.11. *Suppose that $\alpha \in \mathbb{E}$ and $p \in \mathbb{Z}$ is a prime such that $p \mid N(\alpha)$ but p does not divide α . Then α can be written as $\pi\alpha'$ where $N(\pi) = p$, and 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 ring \mathbb{E} is right Euclidean, so the right ideal $R = (\alpha, p)_r$ is generated by an element π . Since $\alpha, p \in R$ we have that π divides both α and p on the left. Write $p = \pi\tau$. Then $N(\pi)N(\tau) = p^2$. If $N(\pi) = p^2$, then τ is a unit, hence p is an associate of π , and therefore p divides α , contradicting our assumption. If $N(\pi) = 1$, then π is a unit, so $\alpha\tau_1 + p\tau_2 = 1$ for some $\tau_1, \tau_2 \in \mathbb{E}$. Thus $\bar{\alpha}\alpha\tau_1 + \bar{\alpha}p\tau_2 = \bar{\alpha}$ showing that $p \mid \bar{\alpha}$. Hence again p divides α , which is a contradiction. The only remaining possibility is that $N(\pi) = p$ (implying that π is an irreducible element of \mathbb{E}). Thus π is a left divisor of α with norm p .

Conversely, if π_1 is a left divisor of α with norm p , then α and $p = \pi_1\bar{\pi}_1$ 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 $(\pi_1)_r = (\pi)_r = (\alpha, p)_r$. \square

Lemma 2.12. *Suppose that $\theta, \eta, \pi \in \mathbb{E}$ such that $N(\pi) = p$ is a prime in \mathbb{Z} . If $\pi \mid \theta$, $p \mid \bar{\theta}\eta$ but p does not divide θ , then $\pi \mid \eta$.*

Proof. By Lemma 2.11, $(p, \theta)_r = (\pi)_r$, that is, $\pi = \theta\tau_1 + p\tau_2$ for some $\tau_1, \tau_2 \in \mathbb{E}$. Hence $\bar{\pi}\eta = \bar{\tau}_1\bar{\theta}\eta + p\bar{\tau}_2\eta$, and as p divides $\bar{\theta}\eta$ we get that $p \mid \bar{\pi}\eta$. Using $p = \bar{\pi}\pi$ this shows that $\pi \mid \eta$. \square

Theorem 2.13. *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 .*

Corollary 2.14. *The number of integral quaternions with norm n is 24 times the sum of positive, odd divisors of n .*

Theorem 2.15 (Jacobi). *Let $\sigma(s)$ denote the sum of positive divisors of any integer s , and for every positive integer n , let N be the number of solutions of the Diophantine equation*

$$x^2 + y^2 + u^2 + v^2 = n \quad (x, y, u, v \in \mathbb{Z}).$$

If n is odd, then $N = 8\sigma(n)$. If $n = 2^t m$, where m is odd and $t > 0$, then $N = 24\sigma(m)$ (see Theorem 386 of [HW79]).

Lemma 2.16. *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 $N(\alpha) = p^\ell$ 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 2.11 shows that α can be written as $\alpha_2\pi_2$, with $N(\pi_2) = p$, where α_2 is unique up to right association, and π_2 is unique up to left association. Apply Lemma 2.12 for $\theta \mapsto \bar{\alpha}$, $\eta \mapsto \pi_1$ and $\pi \mapsto \bar{\pi}_2$. We get that if $\alpha\pi_1$ is divisible by p , then π_2 and $\bar{\pi}_1$ are left associates. Conversely, if π_2 and $\bar{\pi}_1$ are left associates, then clearly $p \mid \alpha\pi_1$.

By Theorem 2.13, 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. \square

3. INTEGRAL EULER MATRICES

In Theorem 1.3 describing primitive icubes Sárközy uses Lipschitz integral quaternions. It will be more convenient in this paper to generate cubic lattices by Hurwitz quaternions. 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 . As Corollary 3.9 Sárközy's theorem is obtained. The proofs are elementary in the sense that decomposition to irreducible quaternions is not used.

We now explain how to permute the columns of an Euler matrix by changing its generating quaternion. By Theorem 1.2, $E(\alpha)$ is the matrix of $R(\alpha) : \beta \mapsto \alpha\beta\bar{\alpha}$, 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) is not necessarily. This problem is averted by taking the negative of an odd number of columns.

Proposition 3.1. *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 $i + j + k$ through 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 $i \in \mathbb{Z}^3$ through an angle of $\pm 90^\circ$ (hence 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. \square

Before going further let us record the action of these isometries on \mathbb{R}^3 .

Proposition 3.2. *Denote by H the group of units of \mathbb{E} (see Proposition 2.9), 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 $R((1+i)/\sqrt{2})$ 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 . \square

The proof is left to the reader. Note that these groups H and G are the so-called binary tetrahedral group and binary octahedral group, respectively.

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

In all cases $N(\alpha)$ 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 will utilize several lemmas. The first one explains the equivalences stated within the theorem.

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

Proof. As β is primitive, it has an odd component. Thus the statement follows from the fact that the square of an odd integer is congruent to 1 modulo 8. \square

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

Proof. By Theorem 1.2, the length of every column and row of $E(\alpha)$ is $N(\alpha)$, which is an integer by Proposition 1.1. Suppose that it is an even number. Let (a, b, c) be a row of $E(\alpha)$. Then taking $a^2 + b^2 + c^2 = N(\alpha)^2$ modulo 4 we see that a, b, c are even. Thus each entry of $E(\alpha)$ is even, violating the condition that $E(\alpha)$ is primitive. Therefore $a^2 + b^2 + c^2 \equiv 1 \pmod{4}$ showing that exactly one of a, b, c is odd. \square

The next lemma contains an elementary proof of the last part of Proposition 2.9 for right associates.

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).*

Proof. Elementary calculation shows that

$$\begin{aligned}\alpha\sigma &= \frac{m - n - p - q + (m + n + p - q)i}{4} \\ &\quad + \frac{(m - n + p + q)j + (m + n - p + q)k}{4} \\ \alpha\sigma^{-1} &= \frac{m + n + p + q + (-m + n - p + q)i}{4} \\ &\quad + \frac{(-m + n + p - q)j + (-m - n + p + q)k}{4}.\end{aligned}$$

By Lemma 3.4 all integers m, n, p, q are odd. Therefore, either $m - n - p - q$ or $m + n + p + q$ is divisible by 4. However, all four integer coefficients in the numerator of $\alpha\sigma$ are congruent to each other modulo 4, and the same is true for $\alpha\sigma^{-1}$, hence one of these two quaternions is a Lipschitz integral quaternion with an odd norm $N(\alpha)$. The components of this quaternion are obviously relatively prime. \square

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

Proof. By Lemma 3.4 exactly two of m, n, p, q are odd. We may assume that m and n have the same parity (dealing with the other two cases is analogous). Thus

$$\alpha = \frac{1 + i}{\sqrt{2}} + \sqrt{2}(a + bi + cj + dk) \quad \text{or} \quad \alpha = j\frac{1 - i}{\sqrt{2}} + \sqrt{2}(a + bi + cj + dk)$$

with $a, b, c, d \in \mathbb{Z}$. Obvious calculation shows that the quaternion $\alpha(1 + i)/\sqrt{2} = \beta$ has integral coefficients and $N(\beta) = N(\alpha)$ is odd. \square

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 1.2 has integral entries and is primitive. By Lemma 3.5 $N(\alpha) = m^2 + n^2 + p^2 + q^2$ is an integer, and the diagonal elements of $E(\alpha)$ are integers, too. 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 also obtain that all the numbers $4mn$, $4mp$, $4mq$, $4np$, $4nq$, and $4pq$ are integers as well. Therefore, the squarefree parts of the non-zero numbers among $4m^2$, $4n^2$, $4p^2$ and $4q^2$ are the same. Denote this common squarefree part by r . The quaternion $\alpha = m + ni + pj + qk$ can be written uniquely in the form

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

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 squarefree 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 $N(\alpha)$ 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 $N(\varepsilon) = 1$ such that $\alpha\varepsilon$ is of type (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 $N(\alpha\varepsilon)$ is odd by assumption, the entries in the main diagonal of $E(\alpha\varepsilon)$ are odd. By way of contradiction, 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 primitivity of $\alpha\varepsilon$. Thus, $E(\alpha\varepsilon) = E(\alpha)E(\varepsilon)$ is indeed a primitive integer matrix.

Finally we 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. Type (2) quaternions are handled by Lemma 3.7, and these correspond to the switch 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. \square

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 iff M is orientation-reversing. The new M can be written as $M = E(\alpha)$ for some quaternion α (with real coefficients), by

Theorem 1.2. This α has one of the three types of Theorem 3.3. Modify α using Proposition 3.1 so that the odd entries move to the main diagonal. Then we get an integral Lipschitz quaternion by the last statement of Theorem 3.3. If this transformation changes the sign of a column other than what has originally been the third, then use Proposition 3.1 to change the sign of two columns back. \square

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 $\delta = \alpha\beta\bar{\alpha}$, where α is a fixed Hurwitz integral quaternion, and β runs over all pure integral quaternions (see Corollary 5.11). The generating icube is given by $\alpha i \bar{\alpha}$, $\alpha j \bar{\alpha}$, $\alpha k \bar{\alpha}$.

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 “accidentally”. 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 with Lipschitz quaternions.

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

Proof. By Lemma 2.11 we get that $\delta = \pi\delta_2$ for some $\pi, \delta_2 \in \mathbb{E}$ such that $N(\pi) = p$. Then $N(\delta) = pN(\delta_2)$, hence p divides $N(\delta_2)$ but p clearly does not divide δ_2 . By the dual of Lemma 2.11 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 $\bar{\delta} = \bar{\pi}_1\bar{\delta}_3\bar{\pi}$. But δ is a pure quaternion, hence $\bar{\delta} = -\delta$. Therefore δ is divisible by π and by $\bar{\pi}_1$ on the left. By the uniqueness statement of Lemma 2.11 we get that π and $\bar{\pi}_1$ are right associates. Thus $\delta = \pi\delta_3\pi_1$ can be written as $\pi\delta_1\bar{\pi}$ indeed. \square

Theorem 4.2. *Let $\delta \in \mathbb{E}$ be a pure quaternion whose norm $N(\delta) = nm^2$. Suppose that no integer prime divisor of m divides δ . Then δ can be written as $\alpha\beta\bar{\alpha}$ for some $\alpha, \beta \in \mathbb{E}$ such that $N(\alpha) = m$ and $N(\beta) = n$. 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 proved by induction on m : apply Lemma 4.1 successively for 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 that $\varepsilon\beta_1\varepsilon^{-1} = \beta_2$. If $m > 1$, then let $p \in \mathbb{Z}$ be a prime divisor of m . Apply Lemma 2.11 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, hence the uniqueness statement of Lemma 2.11 implies that π_1 and π_2 are right associates. So 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. Thus so are $\alpha_1 = \pi_1\alpha_3$ and $\alpha_2 = \pi_1\varepsilon\alpha_4$.

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, and therefore by taking a right associate of α we may choose any of them to be β . \square

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 $N(\alpha) = m$. 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 of 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. \square

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

Proof. The proof is an easy 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 . \square

Lemma 4.5. *Let $\pi, \beta \in \mathbb{E}$ such that β is a pure quaternion and $p = N(\pi) > 2$ 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. First 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 implies 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 in this paragraph. Let

$$\beta_2 = (i\pi)\beta(i\pi)^{-1} = i\beta_1i^{-1},$$

this 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. However, if both π and $i\pi$ are “bad”, that is, $\pi \mid \tau = \beta + \beta_1$ and also $i\pi \mid \beta + \beta_2$, then $\pi \mid i^{-1}\beta i + \beta_1$, and so $\pi \mid \beta - i^{-1}\beta i$. Put $\beta = ai + bj + ck$, then $\beta - i^{-1}\beta i = 2(bj + ck)$. If $j\pi$ and $k\pi$ are “bad”, too, then π divides $2(ai + ck)$ and $2(ai + bj)$ as well. Taking norms we get, using $N(\pi) = p > 2$, that p divides $a^2 + b^2$, $a^2 + c^2$ and $b^2 + c^2$, so p divides a , b , c , and therefore p divides β . Therefore $\overline{\pi} \mid h + \beta$ for $h = 0$, and so we are done in this case. Thus we can 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 $d = N(\tau)$, then $d\tau^{-1}\pi = \overline{\tau}\pi$ centralizes β as well. The centralizer of β consists of the 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 $\overline{\overline{\tau}\pi} = \overline{\tau}\pi$. Write $\overline{\tau}\pi = u + v\beta$, 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 $\overline{\tau}\pi$ need not have integer coefficients).

Next we show that p does not divide $2vd$. Suppose it does. Taking norms we get that $N(\overline{\tau}\pi) = p \mid 4N(u + v\beta) = (2u)^2 + (2vd)^2 N(\beta')$, 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 which are divisible by p . Since $p \neq 2$, we have $u' + v'\beta = (u + v\beta)/p \in \mathbb{E}$ in either case. Then $\overline{\tau}\pi = u + v\beta = p(u' + v'\beta) = \overline{\tau}\pi(u' + v'\beta)$, so $\tau = \pi(u' + v'\beta)$, contradicting our assumption that π does not divide τ on the left. Therefore we indeed 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 $\overline{\pi} \mid x(2u) + \beta'$ so the integer $h = x(2u)d$ works. \square

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 hold.*

- (1) p divides α or β .
- (2) $p = 2$, which does not divide α, β but divides $N(\alpha)$.
- (3) $p > 2$, which does not divide α, β but divides $N(\alpha)$ 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 $N(\alpha)$.

Proof. If (1) holds, then clearly $p \mid \alpha\beta\overline{\alpha}$. If (2) holds, then the dual of Lemma 2.11 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 $N(\alpha)$, then we have $p \mid \overline{\alpha}(\alpha\beta\overline{\alpha})\alpha = N(\alpha)^2\beta$, hence $p \mid \beta$, a contradiction. Hence we

may assume that we are in case (3), that is, $p > 2$ and $p \mid N(\alpha)$. We proceed by induction on $N(\alpha)$. By the dual of Lemma 2.11 $\alpha = \alpha_1\pi$ for some $\alpha_1, \pi \in \mathbb{E}$ with $N(\pi) = p$. We show that $\beta_1 = \pi\beta\bar{\pi}$ is divisible by p . Then we are clearly done by Lemma 4.5.

Suppose to get a contradiction that β_1 is not divisible by p . Apply the induction hypothesis to $\alpha_1\beta_1\bar{\alpha}_1$ (which is equal to $\alpha\beta\bar{\alpha}$). We must be in case (3), since $p > 2$ and p does not divide 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 $\bar{\pi}_1 \mid h_1 + \beta_1$. Taking norms we see that $p = N(\pi_1) \mid N(h_1 + \beta) = h_1^2 + N(\beta_1)$. But $N(\beta_1) = p^2 N(\beta)$ is divisible by p , so $p \mid h_1$, and therefore $\bar{\pi}_1 \mid \beta_1$. Since β_1 is not divisible by p , the uniqueness part of Lemma 2.11 shows that $\bar{\pi}_1$ and π are right associates. But then α is divisible on the right by $\pi_1\bar{\pi}_1 = p$, contradicting our assumptions. \square

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 $\alpha\beta\bar{\alpha}$ that are not divisible by p is*

- (1) ep^ℓ if $p \mid N(\beta)$;
- (2) $e(p^\ell - p^{\ell-1})$ if $-N(\beta)$ 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 $\alpha\beta\bar{\alpha}$ is divisible by p , so suppose that p is odd. Call a pair (α_1, β_1) “good”, if $\alpha_1 \in \mathbb{E}$ with $N(\alpha_1) = p^\ell$, there is a unit $\varepsilon \in \mathbb{E}$ such that $\beta_1 = \varepsilon^{-1}\beta\varepsilon$, and p does not divide $\alpha_1\beta_1\bar{\alpha}_1$. By the uniqueness part of Theorem 4.2 every element $\alpha_1\beta_1\bar{\alpha}_1$ 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 2.11, where π_2 of norm p is uniquely determined up to left association. Theorem 4.6 shows that $\alpha_1\beta_1\bar{\alpha}_1$ is divisible by p if and only if $\bar{\pi}_2$ divides $h + \beta_1$ for some integer h (assuming that α_1 is not divisible by p). Let us count the number of such quaternions π_2 .

Clearly, $\bar{\pi}_2 \mid h + \beta_1$ implies $N(\pi_2) = p \mid N(h + \beta_1) = h^2 + N(\beta_1)$. This means that either $p \mid N(\beta_1)$ or $-N(\beta_1)$ 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 2.11, there is exactly one left divisor $\bar{\pi}_2$ up to right association with norm p of any given $h + \beta_1$ for which $p \mid h^2 + N(\beta_1)$. Thus π_2 is unique up to left association. Clearly, the numbers h_1 and h_2 yield the same $\bar{\pi}_2$ if and only if $h_1 \equiv h_2 \pmod{p}$. If $p \mid N(\beta_1)$, 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

$1 \leq h \leq p - 1$ such that $p \mid h^2 + N(\beta_1)$ (since p is an odd prime, assuming of course that $-N(\beta_1)$ is a quadratic residue mod p). So in this case there are two “bad” values for π_2 up to left association.

By Theorem 2.13 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 $24p^{\ell-1}$ by Lemma 2.16. Since the number of possible β_1 is e , we get the result. \square

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 $m, n \geq 1$ are integers and n is squarefree. 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 do induction on the number of prime divisors of m . Let $m = p^\ell m_1$, 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 $\alpha\beta\bar{\alpha}$, where $N(\alpha) = p^\ell$.

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

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

Corollary 4.9. *Suppose that $m, n \geq 1$ are integers and n is squarefree. 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.

First we translate everything to the language of quaternions. Recall that every vector $v = (v_1, v_2, v_3) \in \mathbb{R}^3$ is identified by the pure quaternion $V(v) = v_1i + v_2j + v_3k$.

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) $N(\theta) = N(\eta)$;
- (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 . \square

Next we translate the construction of twin pairs given in the Introduction. Denote by (u, v, w) the columns of an Euler matrix given by $\alpha \in \mathbb{E}$ (the ring of Hurwitz integral quaternions, see Definition 2.7). By Proposition 2.8 $N(\alpha)$ 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 $V(v)$, k to $V(w)$. It maps the twin quaternions $zj = aj + bk$ and $zk = ak - bj$ to $\alpha zj \bar{\alpha}$ and $\alpha zk \bar{\alpha}$, respectively, which therefore 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 $\theta = \alpha zj \bar{\alpha}$ and $\eta = \alpha zk \bar{\alpha}$. 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 $\alpha_1 z_1 j \bar{\alpha}_1 = \alpha_2 z_2 j \bar{\alpha}_2$ and $\alpha_1 z_1 k \bar{\alpha}_1 = \alpha_2 z_2 k \bar{\alpha}_2$.

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

Proof. Note that $\alpha^{-1} = \bar{\alpha}/N(\alpha)$ and $x \mapsto \alpha x \alpha^{-1}$ is an automorphism of the division ring \mathbb{H} . Therefore $\theta\eta = N(\alpha)\alpha z j z k \bar{\alpha}$. But $z j z k = z j z j^{-1} j k = z \bar{z} i$, so $\theta\eta = N(\alpha)N(z)\alpha i \bar{\alpha}$, which is pure. \square

Theorem 5.4. *The characterization of twin quaternions is 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 squarefree 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 squarefree. 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 squarefree, the number $z \in \mathbb{G}$ is either real or pure imaginary.*

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

Proof. Suppose that p does not divide $\theta\eta$. By Lemma 2.11 and Lemma 4.1 we have $\theta = \pi_1\theta_1$, $\eta = \eta_1\pi_2$ and $\theta\eta = \pi\delta_1\bar{\pi}$, where π, π_1, π_2 have norm p . By the uniqueness part of Lemma 2.11 π, π_1 and $\bar{\pi}_2$ are right associates. However, θ, η and $\theta\eta$ are pure quaternions, so $\theta\eta = -\overline{\theta\eta} = -\bar{\eta}\bar{\theta} = -\eta\theta = -\eta_1\pi_2\pi_1\theta_1$ is divisible by p , a contradiction. \square

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

Proof. By Lemma 5.5 $p \mid \delta = \theta\eta$. Using Lemma 4.1 we can write $\theta = \pi\theta_1\bar{\pi}$ and $\eta = \pi_1\eta_1\bar{\pi}_1$, where $N(\pi) = N(\pi_1) = p$. Since θ is pure, $\delta = \theta\eta = -\bar{\theta}\eta$, so Lemma 2.12 shows that $\pi \mid \eta$. Applying the uniqueness part of Lemma 2.11 to η we obtain that π and π_1 are right associates. \square

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

Proof. Again write $\theta = \pi\theta_1\bar{\pi}$. Suppose first that $\pi \mid \eta$, that is, $\eta = \pi\eta_2$ for some $\eta_2 \in \mathbb{E}$. Then $p\eta = \pi(\eta_2\pi)\bar{\pi}$, so we are done in this case. So we can assume that π does not divide η . Since θ is pure, $\delta = \theta\eta = -\bar{\theta}\eta$, so Lemma 2.12 shows that p does not divide δ . By Lemma 4.1 and the uniqueness part of Lemma 2.11, we have $\delta = \pi\delta_1\bar{\pi}$. Then $\pi\theta_1\bar{\pi}\eta = \delta = \pi\delta_1\bar{\pi}$ implies that $\theta_1\bar{\pi}\eta\pi = \delta_1\bar{\pi}\pi = p\delta_1$. Hence $p \mid \bar{\pi}\eta\pi\theta_1$. Lemma 2.12 shows that either $\bar{\pi} \mid \theta_1$ or $p \mid \bar{\pi}\eta\pi$. The first case is impossible because then θ would be divisible by p . Let $\bar{\pi}\eta\pi = p\eta_1$, then $p\eta = \pi\eta_1\bar{\pi}$. \square

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

Proof. Let $M = N(\theta) = N(\eta)$. Consider all representations of the form $\theta = \alpha\theta_1\bar{\alpha}$ and $\eta = \alpha\eta_1\bar{\alpha}$, 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 $\alpha = 1$), so there is one where $N(\alpha)$ is as large as possible. We present reductions to increase $N(\alpha)$.

If p is a prime such that p^2 divides both $N(\theta_1)$ and $N(\eta_1)$, 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 write $\eta_1 = p^\ell \eta'$ such that η' is not divisible by p , and apply Lemma 5.7 to θ_1 and η' . Then again we obtain a suitable π (by using up a factor of p out of p^ℓ).

If none of these reductions can be performed anymore, then $\theta_1 = d\theta_2$ and $\eta_1 = d\eta_2$ for some $d \in \mathbb{Z}$ such that $N(\theta_2) = N(\eta_2)$ is squarefree. By Lemma 5.5 every integer prime divisor of $N(\eta_2)$ divides $\theta_2\eta_2$. Hence the squarefree number $N(\eta_2)$ divides $\theta_2\eta_2$, whose norm is $N(\eta_2)^2$. Therefore $\theta_2\eta_2 = N(\eta_2)\varepsilon$, where ε is a unit of \mathbb{E} . We may assume that $\varepsilon = i$ 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 $\theta = \alpha(dz_1)j\bar{\alpha}$ and $\eta = \alpha(dz_1)k\bar{\alpha}$, proving the claim. \square

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 $jsj^{-1} = \bar{s}$ for every $s \in \mathbb{C}$, we have that $zj = stj\bar{s}$ and similarly $zk = stk\bar{s}$. Therefore $\alpha z j \bar{\alpha} = (\alpha s) t j (\overline{\alpha s})$ and $\alpha z k \bar{\alpha} = (\alpha s) t k (\overline{\alpha s})$. \square

This lemma immediately implies (2) of Theorem 5.4, and (1) has been proved 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. So we 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 , and it centralizes k , too, 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 $N(\alpha_1)^2 N(s_1)^2 = N(\alpha_2)^2 N(s_2)^2$, hence $N(t) = 1$, and thus $t = \pm 1$.

This implies that $\alpha_1^{-1} \alpha_2 = \rho$ is a complex number, which has rational components. Then $\rho^2 = (s_1 s_2^{-1})^2 = z_1 z_2^{-1}$. Therefore $z_1 z_2 = (\rho z_2)^2$, and Lemma 2.1 implies that $\rho z_2 \in \mathbb{G}$. Since z_1 and z_2 are squarefree, each Gaussian prime divisor of z_1 has multiplicity 1 in both z_1 and z_2 , and the same holds for z_2 . Therefore z_1 and z_2 are associates, and so ρ^2 is a unit in \mathbb{G} . Thus $N(\rho) = 1$, and Lemma 2.1 shows that ρ is in \mathbb{G} , so (3) of Theorem 5.4 is proved.

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

Suppose that $N(z)$ is a square and consider a Gaussian prime divisor π of z . As z is squarefree in \mathbb{G} , the number π^2 does not divide z . Hence $\pi = 1 + i$ is impossible, since all other Gaussian primes have odd norm, and so $N(z)$ would be of the form $4k + 2$. Similarly, if $p = N(\pi)$ is an odd prime (of the form $4k + 1$), then $p \mid N(z)$, and so the conjugate of π must also occur in z . Therefore z is indeed real or pure imaginary, and so the proof of Theorem 5.4 is complete. \square

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

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

where p_1, \dots, p_m are primes $\equiv 1 \pmod{4}$ and q_1, \dots, q_ℓ are primes $\equiv -1 \pmod{4}$; we assume that all λ_r and μ_s are positive. Then

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

where

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

and

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

In particular, $T(M)/24$ 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 $M = N(\alpha)^2 N(z)$ and z is squarefree in \mathbb{G} , and divide the number of solutions by 4 because of (3).

Writing z as a product of Gaussian primes we see that in the canonical form of $N(z)$ 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 $t = N(z)$ is given, then the only freedom in determining z occurs at the primes p of the form $4k + 1$. Indeed, $p = \pi_1 \bar{\pi}_1$ is a product of two Gaussian primes, and if the exponent of p in $N(z)$ is 1, then we can decide whether to put π or $\bar{\pi}$ 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 $p \equiv 1 \pmod{4}$.

Corollary 2.14 allows us to count the number of integral quaternions α with given norm $N(\alpha)$. The result is 24 times a multiplicative function (the sum of odd divisors of $N(\alpha)$). Now we go through all primes in the decomposition of M to see how we can split M into $N(\alpha)^2 N(z)$.

If the prime is 2, then we must put 2^κ into $N(\alpha)^2$ if κ is even, and must put $2^{\kappa-1}$ into $N(\alpha)^2$ if κ is odd. By Corollary 2.14 we see that $T(2^\kappa) = 24$, and $T(M)$ does not depend on κ .

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

Finally for $p_r \equiv 1 \pmod{4}$ there are two cases to consider. If λ_r is even, then we can put 0 or 2 copies of p_r into $N(z)$. If λ_r is odd, then we must put 1 copy of p_r into $N(z)$

(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. \square

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 $(V(v), V(w)) = (\theta, \eta)$, parameterized by (α, z) where z is squarefree. 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 $\theta = d\alpha j \bar{\alpha}$ and $\eta = d\alpha k \bar{\alpha}$, so the last two columns of $dE(\alpha)$ are v and w . In the second case $\theta = d\alpha k \bar{\alpha}$ and $\eta = -d\alpha j \bar{\alpha}$, so the last two columns of $dE(\alpha)$ are $-w$ and v . \square

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 signs of columns.*

Proof. By Proposition 1.1 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, so they share the third column of $E(\alpha)$ as well. \square

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

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

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 primitive, too. 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: $V(x) = \alpha_1 \beta_1 \bar{\alpha}_1 = \alpha_2 \beta_2 \bar{\alpha}_2$. 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 and 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. \square

Proof of Corollary 1.6. We use the notation of the previous proof, let L denote the unique sublattice obtained there. Proposition 3.2 says 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 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) such that z_1 is squarefree. By Lemma 5.13 $N(z_1) = n$, hence $N(\alpha_1) = m$. Thus the sublattice generated by α_1 is L . Since $z_1 j$ has a zero component, in case (1) of Corollary 1.6 the vector x cannot have a twin.

If the norm of x is a square, then $1 = n = N(z_1)$, and therefore $z_1 \in \{\pm 1, \pm i\}$. 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. So $\varepsilon \in Q$. 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. \square

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 $N(\theta) = n$, then 2θ has a twin η , and so $\eta/2$ is a twin of θ . \square

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), $\alpha\beta\bar{\alpha}$ 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). \square

Proof of Theorem 1.8. Let $n, m > 0$ be integers such that n is squarefree. First 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, $\delta = \alpha\beta\bar{\alpha}$ for some $\alpha, \beta \in \mathbb{E}$ such that $N(\alpha) = m$ and $N(\beta) = n$. Since n is twin-complete, β has a twin γ . We show that $\alpha\gamma\bar{\alpha}$ is a twin of δ , using Proposition 5.1. Indeed,

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

This is a pure quaternion, since $\beta\gamma$ is a pure quaternion. So we have proved 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 $\theta = \alpha\beta\bar{\alpha}$ 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 squarefree. Thus $\theta = \alpha_1 z j \bar{\alpha}_1$, so by Lemma 5.13, $N(z)$ is the squarefree part of $N(\theta)$, that is, $N(z) = n$ and $N(\alpha_1) = m$. 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 at most two positive 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 $\beta = \alpha z j \bar{\alpha}$ for some $(\alpha, z) \in \mathbb{E} \times \mathbb{G}$. Here $n = N(\beta) = N(\alpha)^2 N(z)$, so $N(\alpha) = 1$ 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). \square

Now we discuss Conjecture 1.9. Let

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

denote the list of those squarefree numbers that can be written as a sum of at most two positive 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 $n \equiv 2 \pmod{4}$ are given by $xyz = 0$, and when $n \equiv 1 \pmod{4}$ 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 his list is complete ([Rib00]). It was S. Chowla who proved that there are only finitely many *numeri idonei* ([Cho34]). P. J. Weinberger improved Chowla's result to show that if Euler's list is not complete, then at most one *numerus idoneus* is absent and it must be greater than $2 \cdot 10^{11}$ ([Wei73]).

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, squarefree, 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.

7. GEOMETRIC CONSIDERATIONS

Our goal in this section is to shed light on the main results of the paper by using elementary methods. Doing so, we reprove several results in a geometrical way. The vectors that we work with will be assumed to be non-zero, unless otherwise stated.

Our first result strengthens Lemma 5.5 in the case of equally long vectors.

Proposition 7.1. *Let $x, y \in \mathbb{Z}^3$ be two orthogonal vectors of equal norm (length squared) $N(x) = N(y) = nm^2$, where $n, m \in \mathbb{N}$, n is squarefree. We claim that the cross product $x \times y$ is divisible in \mathbb{Z}^3 by nm .*

Proof. Let $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$. Our hypotheses mean that

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 = nm^2 &= y_1^2 + y_2^2 + y_3^2, \\ x_1 y_1 + x_2 y_2 + x_3 y_3 &= 0. \end{aligned}$$

From the second equation we get that $x_3^2 y_3^2 = x_1^2 y_1^2 + x_2^2 y_2^2 + 2x_1 x_2 y_1 y_2$. We compute the square of the third coordinate $x_1 y_2 - x_2 y_1$ of $x \times y$ as follows:

$$\begin{aligned} (x_1 y_2 - x_2 y_1)^2 &= (x_1^2 + x_2^2)(y_1^2 + y_2^2) - x_3^2 y_3^2 \\ &= (nm^2 - x_3^2)(nm^2 - y_3^2) - x_3^2 y_3^2 \\ &= nm^2(nm^2 - x_3^2 - y_3^2). \end{aligned}$$

As n is squarefree, $n^2 m^2$ divides the square $(x_1 y_2 - x_2 y_1)^2$, hence nm divides the third coordinate of $x \times y$. By a similar argument it divides all three coordinates. \square

Corollary 7.2 (The case $n = 1$, reproving 5.11). *If $x, y \in \mathbb{Z}^3$ have length $m \in \mathbb{Z}$ and $x \perp y$, then $x \times y$ is divisible (in \mathbb{Z}^3) by m , hence the vector $(x \times y)/m$ extends the twin pair (x, y) to an icube.* \square

Corollary 7.3 (The case $m = 1$). *If $x, y \in \mathbb{Z}^3$ where $N(x) = N(y) = n$ is squarefree and $x \perp y$, then $x \times y$ is divisible by n . Hence $(x \times y)/n$ is one of the six unit vectors of \mathbb{Z}^3 . In particular, x and y lie in one of the three coordinate planes.* \square

Next we reprove the case of Theorem 1.5 for vectors of integer length by elementary means. This also implies Theorem 1.4. By a ‘‘square sublattice’’ we mean a sublattice generated by a twin pair. Sublattices are subgroups of \mathbb{Z}^3 , and therefore it makes sense to speak about the index of them in the sense of group theory.

Theorem 7.4. *Let $v = (a, b, c)$ be a primitive vector in \mathbb{Z}^3 with integral length ℓ , and let $L = \{x \in \mathbb{Z}^3 \mid x \perp v\}$. Then amongst the square sublattices of L there is a greatest one K (with respect to set inclusion), and the index i of K in L equals ℓ .*

Proof. A non-trivial sublattice of L is square if and only if it is invariant under the 90° rotation R about the vector v . Since the sublattice generated by all R -invariant sublattices of L is again R -invariant, there is a greatest such lattice K .

The vectors $r = (0, -cl, bl)$ and $s = (b^2 + c^2, -ab, -ac)$ in L are of equal length and orthogonal to each other, thus they span a square sublattice of L . The area of the square spanned by the vectors r and s is $\ell^2(b^2 + c^2)$. Denote by K_1 the lattice generated by these vectors. By analogous constructions we obtain two other square sublattices K_2 and K_3 , in which the area of the fundamental square is $\ell^2(c^2 + a^2)$ and $\ell^2(a^2 + b^2)$, respectively. The area of a fundamental parallelogram of L is well-known to be ℓ , thus the indices of the lattices K_i in L are $\ell(b^2 + c^2)$, $\ell(c^2 + a^2)$, and $\ell(a^2 + b^2)$. Our hypothesis $\gcd(a, b, c) = 1$ easily implies that $\gcd(b^2 + c^2, c^2 + a^2, a^2 + b^2) = 1$. (Here we take advantage of the fact that out of the numbers a , b , and c exactly one is odd, since the sum of their squares is a square.) This, in turn, implies that the index i of K in L divides the number $\ell = \gcd(\ell(b^2 + c^2), \ell(c^2 + a^2), \ell(a^2 + b^2))$.

Let the vectors u and w span a fundamental square (of area $i\ell$) of the lattice K . According to Proposition 7.1, the length-square $i\ell$ of the vectors u and w divides the square of each coordinate of the vector $u \times w = iv$, that is, $\ell \mid ia^2$, $\ell \mid ib^2$, and $\ell \mid ic^2$, hence $\ell \mid \gcd(ia^2, ib^2, ic^2) = i$, proving the claim $i = \ell$. \square

Corollary 7.5. *Using the hypotheses of the previous theorem, there exists exactly one cubic sublattice C of \mathbb{Z}^3 containing v as a shortest nonzero vector.*

Proof. The greatest square sublattice K of L has index ℓ in L , hence its shortest vectors share the length ℓ with v , consequently K and the vector v span the required cubic sublattice.

On the other hand, if C is a cubic lattice containing v as a shortest (non-zero) vector, then the orthocomplement lattice K' of v in C is a square sublattice of L with index ℓ , hence K' coincides with the greatest square sublattice K of L . \square

A corollary of Theorem 5.10 is that the norm of twins is the sum of two squares. Here we prove this assertion by elementary means.

Proposition 7.6. *The norm of twin vectors in \mathbb{Z}^3 is the sum of two squares.*

Proof. Let $x, y \in \mathbb{Z}^3$ be twin vectors whose norm is M . Consider the lattice L of all integer vectors $z \in \mathbb{Z}^3$ lying in the plane spanned by x and y , and let R be the rotation through 90° in the plane of L . Set $L' = L \cap R(L)$. Plainly, L' is a non-trivial lattice invariant under the rotation R . Therefore, a shortest non-zero element $z \in L'$ and Rz together span L' . Let ℓ be the length of z . The vector $x \times y$ has integer length M , hence it has a twin w in L' by Corollary 7.5. Since $x, w \in L'$ and L' is spanned by z and Rz , there are integers a, b, c, d such that $\sqrt{M} = \ell\sqrt{a^2 + b^2}$ and $M = \ell\sqrt{c^2 + d^2}$. Dividing these equations and taking squares we get that the integer M is equal to $(c^2 + d^2)/(a^2 + b^2)$, hence, each of its prime factors of form $4k + 3$ occur on an even power. \square

8. PYTHAGOREAN QUADRUPLES

This section claims explicitly the characterization of Pythagorean quadruples, lists the theorems of the paper from which this result follows, and gives another, short, constructive proof using Gaussian integers. Consider the Diophantine equation

$$a^2 + b^2 + c^2 = d^2.$$

It is sufficient to find the primitive solutions, that is, when $\gcd(a, b, c, d) = 1$. Considering this quadratic equation mod 4, we realize that d is odd, and among the integers a, b, c exactly one is odd. We may assume that this number is a .

Theorem 8.1. *The quadruple (a, b, c, d) , where $a^2 + b^2 + c^2 = d^2$, $\gcd(a, b, c) = 1$, a is odd, $d > 0$, possesses exactly four Euler parameterizations*

$$\begin{aligned} a &= m^2 + n^2 - p^2 - q^2, \\ b &= 2(mq + np), \\ c &= 2(-mp + nq), \\ d &= m^2 + n^2 + p^2 + q^2 \end{aligned}$$

with some integers m, n, p, q . By setting $n = q = 0$ we get the usual parameterization of Pythagorean triples (where $b = 0$).

This result is found as formula (11) on page 31 of [Car15]. It obviously follows from the fact that (a, b, c) is contained in a unique cubic lattice (see Theorem 1.5), which has been proved using quaternions in Section 5, and also by geometrical methods in Corollary 7.5.

Lemma 8.2. *Let $x, y \in \mathbb{Z}$ be positive integers. Suppose that $xy = \gamma\bar{\gamma}$ with $\gamma \in \mathbb{G}$ and $\gcd(x, y, \gamma, \bar{\gamma}) = 1$. Then there exist integers $m, n, p, q \in \mathbb{Z}$ such that*

$$\begin{aligned} x &= (m + ni)(m - ni), & \gamma &= (m + ni)(p + qi), \\ y &= (p + qi)(p - qi), & \bar{\gamma} &= (m - ni)(p - qi). \end{aligned}$$

Every such quadruple (m, n, p, q) automatically satisfies that

$$\begin{aligned} m + ni &= \gcd(x, \gamma), \\ p + qi &= \gcd(y, \gamma). \end{aligned}$$

Furthermore, the exact number of such quadruples is four.

Proof. We use the notation $\gcd(\alpha, \beta)$ for Gaussian integers, too. Of course this number is unique only up to multiplication by a unit element of the ring \mathbb{G} . We use \sim to denote associates.

Let $\theta = \gcd(x, \gamma) = m + ni$ and $\eta = \gcd(y, \gamma) = p + qi$. Taking conjugates we get $\gcd(x, \bar{\gamma}) = \bar{\theta}$ and $\gcd(y, \bar{\gamma}) = \bar{\eta}$. Clearly $\gcd(\theta, \bar{\eta}) \mid \gcd(x, y, \gamma, \bar{\gamma}) = 1$. From

$$\frac{x}{\theta} \cdot \frac{y}{\bar{\eta}} = \frac{\gamma}{\theta} \cdot \frac{\bar{\gamma}}{\bar{\eta}}$$

we see that x/θ and $\bar{\gamma}/\bar{\eta}$ divide each other, since $\gcd(x/\theta, \gamma/\theta) = \gcd(y/\bar{\eta}, \bar{\gamma}/\bar{\eta}) = 1$.

Now $\gcd(\theta, \bar{\eta}) = 1$, hence $\bar{\gamma}/\bar{\eta} \sim \gcd(\theta\bar{\gamma}/\bar{\eta}, \bar{\eta}\bar{\gamma}/\bar{\eta}) \sim \gcd(x, \bar{\gamma}) = \bar{\theta}$. Modifying θ by multiplying it with a suitable Gaussian unit we get $\bar{\gamma}/\bar{\eta} = \bar{\theta}$. Then $\gamma = \theta\eta$ and $x \sim \theta\bar{\gamma}/\bar{\eta} = \theta\bar{\theta}$. Both are positive integers, so $x = \theta\bar{\theta}$. Hence $y = \gamma\bar{\gamma}/x = \eta\bar{\eta}$.

Since $\theta = m + ni$ is uniquely determined after fixing one of the four possible values of $\eta = \gcd(y, \gamma)$, we get that the number of all quadruples (m, n, p, q) with the required properties is exactly four, thus completing the proof of the lemma. \square

Proof of Theorem 8.1. Write the Pythagorean quadruple equation as

$$(8.3) \quad \left(\frac{c}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = \frac{d+a}{2} \cdot \frac{d-a}{2}$$

or, equivalently,

$$(8.4) \quad \left(-\frac{c}{2} + \frac{b}{2}i\right) \cdot \left(-\frac{c}{2} - \frac{b}{2}i\right) = \frac{d+a}{2} \cdot \frac{d-a}{2}$$

in \mathbb{G} .

Apply Lemma 8.2 for $x = (d + a)/2$, $y = (d - a)/2$ and $\gamma = -c/2 + (b/2)i$. We must show that $\gcd((d + a)/2, (d - a)/2, -c/2 + (b/2)i, -c/2 - (b/2)i) = 1$.

Suppose that $\delta \in \mathbb{G}$ divides $(d - a)/2$ and $(d + a)/2$. It must then divide a and d . Suppose further that δ also divides $-c/2 + (b/2)i$ and $-c/2 - (b/2)i$. It must then divide their sum, which is $-c$, and their difference, which is bi . Therefore, δ divides a, b and c . By assumption, $\gcd(a, b, c) = 1$, and so we must have $\delta \in \{\pm 1, \pm i\}$.

We may now apply Lemma 8.2 to yield integers m, n, p, q such that

$$\begin{aligned}\frac{d + a}{2} &= (m + ni)(m - ni), \\ \frac{d - a}{2} &= (p + qi)(p - qi), \\ -\frac{c}{2} + \frac{b}{2}i &= (m + ni)(p + qi).\end{aligned}$$

The above equations are easily seen to be equivalent to the conclusion of the theorem. The number of such Euler parameterizations (m, n, p, q) is exactly four according to the last statement of the previous lemma. \square

Remark 8.5. We see from Lemma 8.2 and Theorem 8.1 that in order to determine a set of parameters m, n, p, q for a given quadruple (a, b, c, d) , we need only compute $\gcd((d + a)/2, -c/2 + (b/2)i)$ to yield $m + ni$, and then divide $-c/2 + (b/2)i$ by this result to obtain $p + qi$. If $b = 0$, then $m + ni$ and $p + qi$ can be chosen to be real.

9. PROBLEMS AND CONJECTURES

Problem 9.1 (Main problem). Investigate *construction, counting, extension* for higher dimensional icubes. Describe the possible edge lengths of icubes of a given dimension k in \mathbb{Z}^n , and twin-completeness. Generalize the results in this paper.

We make some remarks and state two conjectures. First note that if the dimension is even, then every vector has a twin:

$$(a, b, \dots, c, d) \quad \text{and} \quad (-b, a, \dots, -d, c)$$

are twins. Therefore odd dimensions seem more interesting.

Call an integral vector *odd* if every component is odd. Looking at the vectors mod 2 we see that if the dimension is odd, then odd vectors do not have a twin.

Conjecture 9.2. Suppose that the dimension $n \geq 5$ is odd. Then every non-odd vector has a twin.

Every odd vector of length \sqrt{d} satisfies that $d \equiv n \pmod{8}$. Therefore the following conjecture is weaker.

Conjecture 9.3. Suppose that the dimension $n \geq 5$ is odd and $d \not\equiv n \pmod{8}$. Then every vector of length \sqrt{d} has a twin.

Since the number of vectors of a given length grows rapidly with the dimension, it may be possible to use analytic methods in investigating these questions.

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.
- [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.
- [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