An application of integral quaternions

Bolyai Institute — Szeged, April 1, 2009

Lee M. Goswick, Emil W. Kiss, Gábor Moussong, Nándor Simányi

Icubes

An *icube* (integral cube) is a sequence $(v_1, \ldots, v_k)$ of nonzero vectors in $\mathbb{Z}^n$ that are pairwise *orthogonal* and have the *same length.* The number k is the *dimension* of the icube.

The subgroup $\{\sum a_i v_i \, : \, a_i \in \mathbb{Z}\}$ is a *cubic lattice* in $\mathbb{Z}^n$.
Terminology: *norm* is length squared, so it is an integer.

Main questions
Construction: describe all icubes with given k and n.
Counting: how many are there with a given length?
Extension: which ones can be extended (by adding vectors, that is, increasing the dimension)?

In the present work, $n = 3$ and $k = 1, 2$. The case $n = 3$ and $k = 3$ was known before.

The case $k = 3$

Observation
If (u, v, w) is an icube in $\mathbb{Z}^3$, then the common length d of u, v, w is an integer.

Proof
The volume of the cube spanned by u, v, w is d^3, but it is also $\det(u, v, w)$, hence d^3 is an integer. But d^2 is also an integer, since $u, v, w \in \mathbb{Z}^3$. Thus $d = d^3/d^2$ is rational, hence it is an integer. □

Definition
Primitive icube: The nk components of $v_1, \ldots, v_k$ are coprime.

It is clearly sufficient to construct all primitive icubes.

The construction of icubes for $k = 3$

Observation (Euler)
For every $m, n, p, q \in \mathbb{Z}$, the columns of $E(m, n, p, q) =$

$$\begin{pmatrix} m^2+n^2-p^2-q^2 & -2mq+2np & 2mp+2nq \\ 2mq+2np & m^2-n^2+p^2-q^2 & -2mn+2pq \\ -2mp+2nq & 2mn+2pq & m^2-n^2-p^2+q^2 \end{pmatrix}$$

yield an icube with edge-length $d = m^2 + n^2 + p^2 + q^2$.

This is called an *Euler-matrix.*

Theorem (A. Sárközy, 1961)
This icube is primitive iff $(m, n, p, q) = 1$ and d is odd. Every primitive icube can be obtained from a suitable Euler-matrix by permuting columns, and by changing the sign of the last column.

Counting icubes for $k = 3$

Corollary (A. Sárközy, 1961)
The number of primitive icubes with edge-length d is

$$f(d) = 8d \prod_{p \text{ prime},\ p\,|\,d} \left(1 + \frac{1}{p}\right)$$

if d is odd, and 0 if d is even. The number of all icubes with edge-length d is $\sum_{k|d} f(k)$.

The proof is an application of the following well-known result.

Theorem (Jacobi)
If d is odd, then the number of solutions of

$$m^2 + n^2 + p^2 + q^2 = d \qquad (m, n, p, q \in \mathbb{Z})$$

is $8\sigma(d)$ (here $\sigma(d)$ is the sum of positive divisors of d).

Extension from $k = 1$ to $k = 3$

Which integral vectors can be put into an icube?

Necessary: The length must be an integer.
Sufficient to deal with *primitive* vectors.
Answer: *All* such vectors. We use the description of *Pythagorean quadruples.*

Theorem (1915 by R. D. Carmichael, may be earlier)
If $a^2 + b^2 + c^2 = d^2$, where $(a, b, c) = 1$ and a is odd, then

$$a = m^2 + n^2 - p^2 - q^2,$$
$$b = 2mq + 2np,$$
$$c = -2mp + 2nq,$$
$$d = m^2 + n^2 + p^2 + q^2$$

for some integers m, n, p, q (the first column of an Euler-matrix).

Extension from $k = 2$ to $k = 3$

Short name for $k = 2$ and $n = 3$
A *twin pair* is an ordered pair of vectors in $\mathbb{Z}^3$ that are orthogonal and have the same length.

Extension: Which twin pairs can be put into an icube?
Necessary: The length must be an integer.
Answer: *All* such pairs. Indeed:

Elementary calculation
If u and v have length d, then $w = (u \times v)/d$ (cross product) is also an integral vector.
Idea:

If $x_1^2 + x_2^2 + x_3^2 = d^2 = y_1^2 + y_2^2 + y_3^2$ and $x_1y_1 + x_2y_2 + x_3y_3 = 0$,
then $x_3^2y_3^2 = x_1^2y_1^2 + x_2^2y_2^2 + 2x_1x_2y_1y_2$, so
$(x_1y_2 - x_2y_1)^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2) - x_3^2y_3^2$ is divisible by d^2.

Extending primitive vectors to twins
From now on, *icube* means a 3-dimensional icube in $\mathbb{Z}^3$.

Let $x \in \mathbb{Z}^3$ whose norm is nm^2, n square-free. Then there exists an icube (u, v, w) with edge length m such that $x = au + bv + cw$ for some $a, b, c \in \mathbb{Z}$. Thus the relative norm of x in this lattice is square-free.

Theorem (GKMS)
If x is *primitive,* then this cubic lattice is unique. If a, b, c are *nonzero,* then x does not have a twin. If exactly *one* of them is zero, then x has two twins. If *two* are zero, then x has four twins, and is contained in exactly four icubes.

Thus if the length of a primitive vector is an integer, then it has 4 twins. Otherwise the number of its twins is 2 or 0.

Constructing twins

Theorem (GKMS)
If (u, v, w) is an icube and $a, b \in \mathbb{Z}$, then $(av + bw, -bv + aw)$ is a twin pair. We get *all* twin pairs this way. In particular, *the norm of twins is the sum of two squares.*

Problem: this decomposition is not unique.

Bad example
$3(8, -10, 9)$ and $7(4, 5, 2)$ are twins. Neither of them is primitive (this is the main problem). The "right" cubic lattice for them is given by $E(0, 2, 1, 4)$,
that is $u = (-13, 4, 16)$, $v = (4, -19, 8)$, $w = (16, 8, 11)$ with $a = 2$ and $b = 1$.

How to "foresee" the "divisors" of a non-primitive $au + bv + cw$?

Counting twins

Theorem (GKMS)
Denote by $\mathrm{T}(M)$ the number of twin pairs whose norm (length squared) is M. Suppose that

$$M = 2^{\kappa} p_1^{\lambda_1} \dots p_m^{\lambda_m} q_1^{\mu_1} \dots q_\ell^{\mu_\ell} \qquad \big(p_r \equiv 1\ (4), q_s \equiv -1\ (4)\big)$$

(where p_r and q_s are primes and $\lambda_r, \mu_s > 0$), then

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

where

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

In particular, $\mathrm{T}(M)/24$ is a multiplicative function.

Proof: using integral quaternions.

Geometry and quaternions

Well-known in geometry
Identify $(x_1, x_2, x_3) \in \mathbb{R}^3$ and the pure quaternion $x_1 i + x_2 j + x_3 k$.
Let $\alpha = m + ni + pj + qk$ with $\mathrm{N}(\alpha) = m^2 + n^2 + p^2 + q^2 = 1$,
and for $\theta = x_1 i + x_2 j + x_3 k$ let $E(\alpha) : \theta \mapsto \alpha\theta\alpha^{-1} (= \alpha\theta\overline{\alpha})$.
Then $E(\alpha)$ yields a rotation of $\mathbb{R}^3$ whose matrix is $E(m, n, p, q)$.
Conversely, every rotation (element of the group SO($\mathbb{R}^3$)) can be obtained in such a way, and α is unique up to sign.

Example
Let $\alpha = 2i + j + 4k$, its norm is 21. Then $\theta \mapsto \alpha\theta\overline{\alpha}$ is a *dilated rotation*.
It transforms the "planar" twin pair $(2j + k, -j + 2k)$ (norm 5)
to the twin pair $(24i - 30j + 27k, 28i + 35j + 14k)$ (norm $21^2 \cdot 5$).

Hurwitz integral quaternions

Well-known in algebra
Let $\mathbb{E}$ denote the ring of *Hurwitz-quaternions*, that is,
quaternions $a + bi + cj + dk$ such that a, b, c, d are either all integers, or all of them is the half of an odd integer.
Then $\mathbb{E}$ has "unique" factorization (it is right Euclidean).
$\mathbb{E}$ has 24 units ($\sigma = (1 + i + j + k)/2$ is one).
The *irreducible* elements of $\mathbb{E}$ are the ones with *prime norm*.
There are $24(p+1)$ such elements whose norm is $p > 2$, and the elements with norm 2 are the 24 associates of $1 + i$.

It is usually sufficient to use the following for *uniqueness*:

If a prime p divides $\mathrm{N}(\alpha)$ but does not divide α, then $\alpha = \pi\alpha'$ for some π with norm p, and π is unique up to right association.

Decomposing single vectors
Every pure quaternion $\theta \in \mathbb{E}$ can be written as $\alpha\beta\,\overline{\alpha}$, where $\mathrm{N}(\beta)$ is the square-free part of $\mathrm{N}(\theta)$ (and $\alpha \in \mathbb{E}$). If θ is *primitive*, then α is unique up to right associates.

Lemma (GKMS)
If $\alpha\beta\,\overline{\alpha}$ is divisible by an odd prime p, but α and β is not, then $p \mid \mathrm{N}(\alpha)$, and there is an integer h and a right divisor π of α such that $\mathrm{N}(\pi) = p$ and $\overline{\pi} \mid h + \beta$.

Let $s(M)$ denote the number of vectors with norm M. This lemma reduces its computation to the square-free case.

Corollary used for twin-completeness later
For every primitive pure $\beta \in \mathbb{E}$ and $m > 0$ there is an $\alpha \in \mathbb{E}$ with norm m such that $\alpha\beta\,\overline{\alpha}$ is primitive.

Constructing twin pairs

For $u, v \in \mathbb{Z}^3$ let θ, η be the corresponding pure quaternions.
Then $u \perp v$ *iff* $\theta\eta$ is also a pure quaternion.
Let $\alpha \in \mathbb{E}$ and $z \in \mathbb{G}$ (Gaussian integers). Then $\theta = \alpha z j\,\overline{\alpha}$ and $\eta = \alpha z k\,\overline{\alpha}$ are obviously twins.
We say that (θ, η) is *parameterized by* $(\alpha, z) \in \mathbb{E} \times \mathbb{G}$.

Theorem (GKMS)
Each twin pair is parametrized by some pair in $\mathbb{E} \times \mathbb{G}$, where the second component is *square-free* in $\mathbb{G}$.
Such $(\alpha_1, z_1), (\alpha_2, z_2) \in \mathbb{E} \times \mathbb{G}$ yield the same twin pair iff 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 $z_1 = \rho^2 z_2$.

We get an icube exactly when z is real or pure imaginary.

Twin-complete numbers

Recall
A vector can be put into an icube iff its norm is a square.

Extension: Which non-primitive vectors have a twin?

Necessary: The norm must be the sum of two squares.

Easier Problem
Characterize those numbers M such that *every integral vector of norm M has a twin*.

Exclude those M for which there is no vector of norm M (that is, numbers M of the form $4^n(8k + 7)$).

Such numbers M are called *twin-complete*.

Characterizing twin-completeness

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

The proof uses the machinery built above.

Famous conjecture in number theory
The complete list of positive square-free integers that can be written as a sum of two squares, but not as a sum of three *positive* squares, is the following:
$1, 2, 5, 10, 13, 37, 58, 85, 130$.

If true, then d^2, $2d^2$, $5d^2$, $10d^2$, $13d^2$, $37d^2$, $58d^2$, $85d^2$, $130d^2$ are exactly the twin-complete numbers.

Euler's *numeri idonei*

Euler defined a *numerus idoneus* to be an integer n such that, for any positive integer m, if $m = x^2 + ny^2$, $(x^2, ny^2) = 1$, $x, y \geq 0$ has a unique solution, then m is a prime power, or twice a prime power.

Euler's conjecture: his list of 65 *numeri idonei* is complete.
Every number in the conjecture above is a *numerus idoneus.*
Relationship: positive solutions of $xy + xz + yz = n$.
S. Chowla: there are only *finitely many numeri idonei.*
P. J. Weinberger: *At most one square-free number can be missing* from Euler's list, and it is greater than $2 \cdot 10^{11}$ (the largest number on Euler's list is 1848).
If the Generalized Riemann Hypothesis holds, then the possible missing tenth number on the twin-complete list is odd.

Problems in higher dimensions
Study construction, counting, extension for general icubes.
Obvious: In even dimensions n, every vector has a twin.
So suppose that the dimension is odd. What are the possible norms of twins? What about twin-completeness?
Call a vector *odd*, if each of its components is odd.
Obvious: In odd dimensions, odd vectors cannot have a twin.

Conjecture (may be easy!)
Suppose that the dimension $n \geq 5$ is odd. Then every non-odd vector has a twin.

Obvious: Every odd vector of norm M satisfies that $M \equiv n \ (8)$.

Weaker conjecture
Suppose that the dimension $n \geq 5$ is odd and $M \not\equiv n \ (8)$. Then every vector of norm M has a twin.