Cubic lattices

An icube (integral cube) is an ordered triple of vectors in $\mathbb{Z}^3$ that are pairwise orthogonal and have the same length.

If $(u, v, w)$ is an icube, then $\{au + bv + cw : a, b, c \in \mathbb{Z}\}$ yields a cubic lattice in $\mathbb{Z}^3$.

**Observation**

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.

Euler-matrix

**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 $d = m^2 + n^2 + p^2 + q^2$.

Call an icube primitive if the nine components are coprime.

**Theorem (A. Sárközy, 1961)**

$E(m, n, p, q)$ 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 rows, columns, and by transposing.
Counting icubes

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
\[ m^2 + n^2 + p^2 + q^2 = d \quad (m, n, p, q \in \mathbb{Z}) \]
is $8\sigma(d)$ (here $\sigma(d)$ is the sum of positive divisors of $d$).

Pythagorean quadruples

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. Indeed:

Theorem (known since 1915 at least)
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).

Twin vectors

A twin pair is an ordered pair of vectors in $\mathbb{Z}^3$ that are orthogonal and have the same length.

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 $w = (u \times v)/d$ (vectorial 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 $d^2$. 

2
Counting twin pairs

**Theorem (GKMS)**

Denote by $T(M)$ the number of twin pairs whose norm (length squared) is $M$. Suppose that

$$M = 2^k p_1^{\lambda_1} \cdots p_m^{\lambda_m} q_1^{\mu_1} \cdots q_\ell^{\mu_\ell} \quad (p_r \equiv 1 \pmod{4}, q_s \equiv -1 \pmod{4})$$

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

$$T(M) = 24 \prod_{r=1}^m g(p_r^{2\lambda_r}) \prod_{s=1}^\ell h(q_s^{2\mu_s}),$$

where

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

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

In particular, $T(M)/24$ is a multiplicative function.

**Proof:** using integral quaternions.

**Examples of twins**

**Corollary**

If $(u, v)$ is a twin pair, then their norm is the sum of two squares.

**Example**

Let $p$ be a prime of the form $4k + 1$. Then $T(p) = 48$.

These come from its decomposition to the sum of two squares.

If $p = 661$, then $(0, 6, 25)$ has two twins: $\pm(0, 25, -6)$, but $(2, 9, 24)$, $(6, 7, 24)$, $(6, 15, 20)$, $(9, 16, 18)$ have no twins. (There are 216 vectors: change signs, permute coordinates.)

This example shows that there are no “unexpected” twin pairs whose norm is a prime (or squarefree): they all come from decompositions to two squares.

**Decomposing twins**

**Example**

Let $M = 90$. Then $(-4, 7, 5)$ and $(8, 1, 5)$ are (primitive) twins. How can we understand them?

The columns of $E(1, 1, 1, 0)$ yield the cubic lattice

spanned by $u = (1, 2, -2), v = (2, 1, 2), w = (2, -2, -1)$.

The norm here is 9, write $90/9 = 10 = 1^2 + 3^2$. Then $(1, -3)$ and $(3, 1)$ are twins in $\mathbb{Z}^2$, the norm is 10. Combining these we get the twins $1v - 3w$ and $3v + 1w$. These are exactly $(-4, 7, 5)$ and $(8, 1, 5)$.

*It can be proved that this kind of decomposition always exists.*

**Bad example**

Non-primitive $(0, 41, 82)$ has a primitive twin $(60, -62, 31)$. The norm is $41^2 \cdot 5$.  

3
Geometry and quaternions

Well-known in geometry
Identify \((x_1, x_2, x_3) \in \mathbb{R}^3\) with the pure quaternion \(x_1i + x_2j + x_3k\).

Let \(\alpha = m + ni + pj + qk\) with \(N(\alpha) = m^2 + n^2 + p^2 + q^2 = 1\),
and for \(\theta = x_1i + x_2j + x_3k\) let \(E(\alpha) : \theta \mapsto \alpha \theta \alpha^{-1} (= \alpha \theta \alpha)\).
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 \(\text{SO}(\mathbb{R}^3)\)) can be obtained in such a way, and \(\alpha\) is unique up to sign.

\(\alpha = 1 + i + j\), its norm is 3. Then \(\theta \mapsto \alpha \theta \alpha^{-1}\) is a dilated rotation. It transforms the “planar” twin pair \((j - 3k, 3j + k)\) to the twin pair \((-4i + 7j + 5k, 8i + j + 5k)\).
\(\alpha = 6 + j + 2k\) of norm 41 transforms \((j + 2k, -2j + k)\) to the twin pair \((41j + 82k, 60i - 62j + 31k)\).

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 \(N(\alpha)\) but does not divide \(\alpha\), then \(\alpha = \pi \alpha'\) for some \(\pi\) with norm \(p\), and \(\pi\) is unique up to right association.

Decomposing single vectors

Theorem (easy, using Hurwitz-quaternions)
Every primitive, pure quaternion \(\theta\) can be written as \(\alpha \beta \overline{\alpha}\), where \(N(\beta)\) is the square-free part of \(N(\theta)\). Here \(\alpha\) is essentially unique (= up to right associates).

Geometrically: Every primitive vector is contained in a unique cubic lattice such that its relative norm is square-free.

Theorem (GKMS)
A primitive \(\theta\) has a twin iff one of the three components of the corresponding \(\beta\) is zero.

If the length of a primitive integral vector is an integer, then it has exactly 4 twins. Otherwise the number of its twins is 2 or 0.
Parametrizing twin pairs

For $u, v \in \mathbb{Z}^3$ let $\theta, \eta$ 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 $\theta = \alpha z j \bar{\alpha}$ and $\eta = \alpha z k \bar{\alpha}$ are obviously twins.

We say that $(\theta, \eta)$ 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.

Which (not necessarily 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 square-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**

**Obvious:** In even dimensions, 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 $M \neq n \ (8)$. Then every vector of norm $M$ has a twin.

Solve the analogous questions for icubes.