Cuboid Miscellany

Terry Raines
2114 Morning Road
Dyersburg, TN 38024

1. Pythagorean Body Cuboids

Let $p = a^2 + b^2$, $q = a^2 - b^2$, $r = 2ab$, $s = c^2 + d^2$, $t = c^2 - d^2$, and $u = 2cd$. We restrict (a, b, c, d) with the conditions $\gcd(a, b) = \gcd(c, d) = 1$, $a-b$ odd, $c-d$ odd, $b < a$, and $d < c \le a$; also if $c = a$ then $d < b$. These restrictions avoid many trivial repetitions and thus allow the computer program to run faster.

Case I. If $q^2u^2 + r^2t^2$ is a perfect square, the computer finds the dual body cuboids (qu, ru, rt) and (qu, qt, rt) and stores them in a hard disk data file after reducing them to primitives. The generators (a, b, c, d) are also stored in the data file.

Case II. If $q^2t^2 + r^2u^2$ is a perfect square, the dual body cuboids (qt, rt, ru) and (qt, qu, ru) are likewise reduced to primitives and stored in the same hard disk file along with the generators (a, b, c, d).

More explicitly, if we let $\alpha = \sqrt{x^2 + y^2}$, $\beta = \sqrt{y^2 + z^2}$, and $\gamma = \sqrt{x^2 + z^2}$ be the three face diagonals, we obtain the following table.

Case	x	y	z	α	β	$\gamma^2 = x^2 + z^2$
Ia	qu	ru	rt	pu	rs	$q^2u^2 + r^2t^2$
Ib	qu	qt	rt	qs	pt	$q^2u^2 + r^2t^2$
IIa	qt	rt	ru	pt	rs	$q^2t^2 + r^2u^2$
IIb	qt	qu	ru	qs	pu	$q^2t^2 + r^2u^2$

The pursuit of all cases is justified, since we are interested in finding as many different body cuboids as possible. A cuboid found quite early in one case may take quite a long time to be found by another case. The next table gives the counts of body cuboids found by these cases, where each entry under "10^k" is the number of primitive body cuboids with all three edges less than 10^k. The column headed "Total" gives the total count including repetitions; all the other counts exclude repetitions.

$a \le$	Total	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}	10^{16}
1000	7338	698	1706	3027	4128	4704	4872	4874			
2000	15452	704	1844	3972	6601	8700	9888	10337	10356		
3000	23478	704	1869	4297	8065	11682	14133	15418	15842	15846	
4000	31492	704	1877	4433	8946	13871	17761	20031	21116	21248	
5000	39242	704	1880	4506	9467	15558	20786	24231	26050	26550	
6000	46716	704	1880	4544	9822	16901	23358	27958	30547	31602	31640

Recall from Section 1 that the exact numbers of primitive body cuboids with all edges less than 10^7, 10^8, 10^9, and 10^{10} are 704, 1884, 4631, and 10932 respectively.

Despite their apparent similarities, Cases I and II produce quite different cuboids, although both cases will eventually find all primitive body cuboids. For $a \le 1000$ Cases

Ia and Ib each produce 2287 cuboids, while their intersection contains 1232 cuboids; thus Case I produces 3342 different cuboids. On the other hand, Cases IIa and IIb each produce 1382 cuboids, but their intersection is empty; thus Case II produces 2764 different cuboids. The intersection I $\cap$ II contains 1232 cuboids, the same number as Ia $\cap$ Ib. This curious fact is true for any range of the parameter a.

2. Face Cuboid Duals and Pentads

Let $\mathcal{FC}$ be the family of all face cuboids (x, y, z) such that the diagonal $b = \sqrt{x^2 + z^2}$ is not necessarily an integer; that is,

$$\mathcal{FC} = \left\{ (x, y, z) : x^2 + y^2 = c^2,\ y^2 + z^2 = a^2,\ x^2 + y^2 + z^2 = d^2 \right\}$$

where x, y, z, c, a, d are all positive integers. If we define $F_1(x, y, z) = (ay, xy, xz)$ we see that $F_1 : \mathcal{FC} \longrightarrow \mathcal{FC}$ since $(ay)^2 + (xy)^2 = (dy)^2$, $(xy)^2 + (xz)^2 = (ax)^2$, and $(ay)^2 + (xy)^2 + (xz)^2 = (ac)^2$. When we iterate this transformation we find that

$$F_1^2(x, y, z) = F_1(ay, xy, xz) = (xy \cdot ax, ay \cdot xy, ay \cdot xz) = cxy(x, y, z) \ \approx\ (x, y, z)$$

where "$\approx$" means that the two cuboids reduce to the same primitive cuboid. Hence it is natural to call $F_1(x, y, z) = (ay, xy, xz)$ the *face dual* of (x, y, z).

John Leech was the first to note that face cuboids always occur in cycles of five, and in his 1977 paper **[20]** he explained this by citing some technical results on recursive sequences due to Lyness (1942) and Coxeter (1971). Here is a simpler explanation: if we let $F_2(x, y, z) = (xz, xy, ay)$ be the "reverse" of F_1 we find that $F_2 : \mathcal{FC} \longrightarrow \mathcal{FC}$ also, and that $F_2^2(x, y, z) \approx (az, xz, dy)$, $F_2^3(x, y, z) \approx (dy, xz, cx)$, $F_2^4(x, y, z) \approx (cy, yz, xz)$, and $F_2^5(x, y, z) \approx (x, y, z)$. Thus $\left\{ F_2\,,\ F_2^2\,,\ F_2^3\,,\ F_2^4\,,\ F_2^5 \right\}$ is the cyclic group of order five, and so any face cuboid immediately generates four other face cuboids. I call these cyclic groups *pentads*; it is easy to verify that the face dual of any cuboid in a pentad remains in that pentad. More explicitly we have the following identities

	X	Y	Z	D	C	A	B^2	$F_1(X, Y, Z)$
(1)	x	y	z	d	c	a	$x^2 + z^2$	(ay, xy, xz)
(2)	xz	xy	ay	ac	ax	dy	$c^2z^2 + y^4$	$xy(dy, xz, az)$
(3)	az	xz	dy	ad	dz	ac	$x^2y^2 + a^4$	$az(cx, xz, dy)$
(4)	dy	xz	cx	cd	ac	dx	$x^2y^2 + c^4$	$dx(xz, yz, cy)$
(5)	cy	yz	xz	ac	dy	cz	$a^2x^2 + y^4$	$cyz(z, y, x)$

where $A^2 = Y^2 + Z^2$, $B^2 = X^2 + Z^2$, $C^2 = X^2 + Y^2$, and $D^2 = X^2 + Y^2 + Z^2$.

There seems to be no concept of dual for edge cuboids.

3. Pythagorean Face Cuboids

We continue to use the same notation for (p, q, r, s, t, u) as well as

$$\delta = \sqrt{x^2 + y^2 + z^2}$$

for the body diagonal, and we introduce R as the square root of seven special expressions. When the computer determines that R is an integer, we immediately compute the pentad for (x, y, z).

Case	R^2	x	y	z	α	β	δ
I	$p^2u^2 + r^2t^2$	qu	ru	rt	pu	rs	R
II	$q^2s^2 + r^2t^2$	qu	qt	rt	qs	pt	R
III	$p^2t^2 + r^2u^2$	qt	rt	ru	pt	rs	R
IV	$q^2s^2 + r^2u^2$	qt	qu	ru	qs	pu	R
V	$q^2t^2 - r^2u^2$	R	ru	rt	qt	rs	pt
VI	$q^2u^2 - r^2t^2$	R	rt	qt	qu	pt	qs
VII	$r^2t^2 - q^2u^2$	R	qu	ru	rt	pu	rs

There is an eighth case excluded from the preceding table: $R^2 = r^2u^2 - q^2t^2$ never produces face cuboids, because it is the difference between an even square and an odd square, and hence cannot be a perfect square since it is congruent to 3 modulo 4. We use exactly the same restrictions on a, b, c, d as for body cuboids.

$a \le$	Total	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{13}
500	9885	5	27	96	282	746	1554	2518	3383	3936	4222	4426
1000	21570	5	27	96	282	773	1860	3580	5458	7098	8393	8951
1500	33370	5	27	96	282	778	1948	4081	6859	9528	11917	13381
2000	44675	5	27	96	282	779	1981	4358	7839	11438	14728	18679
2500	55975	5	27	96	282	779	1994	4515	8501	12972	17165	20854
3000	67235	5	27	96	282	779	2002	4609	9003	14304	19468	24079
3500	78385	5	27	96	282	779	2010	4686	9420	15431	21495	26982

$a \le$	10^{14}	10^{15}	10^{16}	10^{17}	10^{18}	10^{19}	10^{20}	10^{21}	10^{22}
500	4591	4694	4744	4750					
1000	9411	9745	9977	10164	10225				
1500	14226	14836	15276	15632	15859	15970			
2000	19612	20314	20831	21206	21491	21590			
2500	23029	24318	25311	26027	26568	27011	27261	27295	
3000	27371	29005	30305	31248	31963	32536	32958	33120	
3500	31373	33498	35146	36319	37197	37879	38448	38773	38795

Note that many of the face cuboids found are much larger than the body cuboids in Section 9. This is easily explained: in any pentad three of the face cuboids are $O(a^4)$ and the other two are $O(a^6)$. For example, the five face cuboids in the Case I pentads are (qu, ru, rt), (qt, qu, rs), (pu, rt, qt), (rst, qtu, uR), and (rR, qrt, pqu).

Considering there are seven sets of pentads (35 formulas in all) it is surprising that there are so few repetitions: indeed 38795/78385 $\approx$ 49.5%. For $a \le 1000$ we have the following counts, which include all cuboids in each pentad. As usual, repetitions have been removed except for the Total column.

Case	Total	10^3	10^4	10^5	10^6	10^7	10^8	10^{10}	10^{12}	10^{14}	10^{16}	10^{18}
I	4670	5	27	93	259	583	1084	2281	3131	3418	3649	3725
II	2890	5	26	92	260	535	996	2046	2640	2875	2883	2840
III	3600	5	21	69	195	444	859	1931	2760	2988	3151	3295
IV	2750	0	13	52	166	388	753	1711	2253	2443	2539	2560
V	1560	5	26	94	263	510	834	1369	1525	1551	1560	
VI	3500	5	26	93	256	553	978	1773	2101	2161	2165	
VII	2600	3	19	77	214	431	778	1446	1803	1855	1860	

Note that Cases III, IV, and VII will not find all primitive face cuboids, even though pentads are included. For $a \leq 1000$ we also have the following intersection counts for the seven cases.

	I	II	III	IV	V	VI	VII
I	3725	830	785	845	945	1090	1035
II	830	2890	1070	775	710	1245	1005
III	785	1070	3925	295	770	1170	640
IV	845	775	295	2560	710	760	990
V	945	710	770	710	1560	1010	770
VI	1090	1245	1170	760	1010	2165	745
VII	1035	1005	640	990	770	745	1860

4. Pythagorean Edge Cuboids

The restrictions on (a, b, c, d) are exactly the same as for body and face cuboids. There are apparently twelve cases which must be considered. First we use $\delta = ps$ for the body diagonal and $Z = \delta^2 - x^2 - y^2$ for the square of the irrational side. Since $\beta^2 = \delta^2 - x^2$ and $\gamma^2 = \delta^2 - y^2$ we have

Case	x	y	δ	γ	β	$\alpha^2 = x^2 + y^2$
I	rs	pu	ps	pt	qs	$r^2s^2 + p^2u^2$
II	qs	pt	ps	pu	rs	$q^2s^2 + p^2t^2$
III	qs	pu	ps	pt	rs	$q^2s^2 + p^2u^2$
IV	rs	pt	ps	pu	qs	$r^2s^2 + p^2t^2$

so that $(x, y, \sqrt{Z})$ is an edge cuboid whenever $\alpha = \sqrt{x^2 + y^2}$ is an integer. There are no other possible cases with $\delta = ps$. Actually, Case II cannot occur since $q^2s^2 + p^2t^2$ is never a perfect square: this is because the restrictions on a, b, c, d force q, s, p, t to be odd, so that $\alpha^2 = q^2s^2 + p^2t^2 \equiv 2 \mod 4$, which is impossible.

For the remaining eight cases we note that the four diagonal conditions

$$x^2 + y^2 = \alpha^2 \ , \quad x^2 + Z = \beta^2 \ , \quad y^2 + Z = \gamma^2 \ , \quad x^2 + y^2 + Z = \delta^2$$

are equivalent to the conditions $x^2 + y^2 = \alpha^2$ and $x^2 + \gamma^2 = \delta^2 = y^2 + \beta^2$ from which we can construct the rest of the table:

Case	x	y	α	β	δ	$\gamma^2 = \delta^2 - x^2$
V	rt	qt	pt	qu	qs	$q^2s^2 - r^2t^2$
VI	ru	qu	pu	qt	qs	$q^2s^2 - r^2u^2$
VII	qt	rt	pt	ru	rs	$r^2s^2 - q^2t^2$
VIII	qu	ru	pu	rt	rs	$r^2s^2 - q^2u^2$
IX	qu	qt	qs	rt	pt	$p^2t^2 - q^2u^2$
X	ru	rt	rs	qt	pt	$p^2t^2 - r^2u^2$
XI	qt	qu	qs	ru	pu	$p^2u^2 - q^2t^2$
XII	rt	ru	rs	qu	pu	$p^2u^2 - r^2t^2$

Since $r^2s^2 - q^2t^2$ and $p^2u^2 - q^2t^2$ are congruent to 3 modulo 4 under our restrictions on a, b, c, d, we do not compute Cases VII and XI; hence there are really only nine cases.

Sooner or later these nine search formulas will find all edge cuboids, real or imaginary. In the next two tables, the counts under each column 10^k are the number of primitive edge cuboids, without repetitions, such that $\max(x, y, \sqrt{|Z|}) \leq 10^k$.

Real Edge Cuboids: $\mathbf{Z > 0}$

$a \leq$	Total	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}
500	1432	50	163	389	697	902	1010	1032				
1000	3099	50	174	440	980	1558	1935	2122	2181			
1500	4649	50	174	460	1087	1950	2632	3057	3257	3303		
2000	6173	50	174	474	1141	2177	3169	3861	4196	4356	4365	
2500	7690	50	174	481	1175	2335	3623	4599	5114	5402	5455	
3000	9202	50	174	489	1205	2460	4004	5255	5958	6386	6519	
3500	10675	50	174	490	1223	2564	4309	5826	6726	7287	7528	7542

Imaginary Edge Cuboids: $\mathbf{Z < 0}$

$a \leq$	Total	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}
500	1115	54	151	329	555	683	761	777				
1000	2333	54	155	355	763	1198	1449	1599	1620	1631		
1500	3463	54	155	368	829	1483	1971	2255	2391	2419		
2000	4557	54	155	371	857	1632	2393	2859	3083	3189	3199	
2500	5581	54	155	375	872	1717	2720	3303	3714	3907	3939	
3000	6692	54	155	378	854	1793	2997	3898	4346	4644	4729	4730
3500	7732	54	155	378	897	1848	3183	4337	4948	5334	5499	5505

Examining the nine cases separately, we have the following counts for $a \leq 1000$.

Case	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}	10^{13}
I	0	4	14	39	141	222	341	474	554	598	614	617
III	1	2	5	29	92	140	232	328	391	431	436	
IV	0	0	8	36	94	175	290	387	460	497	504	
V	0	0	7	26	70	162	300	437	505	527	534	
VI	0	1	5	12	49	117	228	353	434	492	527	
VIII	1	3	15	44	138	323	638	429	1025	1077	1082	
IX	1	2	6	39	117	185	306	391	445	465	469	
X	0	3	9	27	92	149	247	335	380	397	398	
XII	0	3	12	60	190	352	571	722	808	857	867	
Total	1	6	27	104	329	795	1743	2756	3384	3721	3809	3812

It is noteworthy that within each of the nine cases there are no repeated cuboids. Of course the row headed "Total" would contain repetitions if we sum the counts in the nine cases, but the counts shown in this row exclude any repetitions. The next table lists the count intersections for $a \leq 1000$; note that Cases I, III, IV, and VI are pairwise disjoint.

	I	III	IV	V	VI	VIII	IX	X	XII
I	617	0	0	0	164	153	0	142	200
III	0	436	0	72	0	149	133	0	56
IV	0	0	504	166	0	80	86	0	172
V	0	72	166	534	0	152	0	0	86
VI	164	0	0	0	527	101	0	0	63
VIII	153	149	80	152	101	1082	77	52	0
IX	0	133	86	0	0	77	469	0	142
X	142	0	0	0	0	52	0	398	137
XII	200	56	172	86	63	0	142	137	865

5. HK Body Cuboids

In 2004 I discovered a new parametric system for body cuboids: for any rational number t the edges are the rational numbers

$$\begin{aligned} x &= 8t(t-1)(t+1)(t+3)(t-5)(t+5)(3t+5)\ , \\ y &= (t-1)(t+3)(t-5)(3t+5)(t^2+2t+5)(t^2+10t+5)\ , \\ z &= 4(5-t^2)(t^2+2t+5)^2(t^2+10t+5)\ . \end{aligned}$$

In 1988 Andrew Bremner [**3**] found five similar systems using elliptic curve methods. Parametric systems can generate 100 million primitive body cuboids per hour since there is no searching for exact squares, but *no known parametric system will generate all possible body cuboids*; indeed they can only find a tiny fraction of them.

My system was based on a 1772 Euler identity (see [**10**], pages 634–635) found in his posthumous papers. Taking $x = pr$, $y = ps$, $z = qs$ with $p = a^2 - b^2$, $q = 2ab$, $r = c^2 - d^2$, $s = 2cd$ ensures that $x^2 + y^2$ and $y^2 + z^2$ are both perfect squares. The square of the third diagonal is $x^2 + z^2 = p^2r^2 + q^2s^2 = A^2c^4 + Bc^2d^2 + A^2d^4$ where $A = a^2 - b^2$ and $B = 20a^2b^2 - 2a^4 - 2b^4$. In 1772 Euler observed that

$$A^2c^4 + Bc^2d^2 + A^2d^4 = \left(Ad^2 + c^2\sqrt{A^2+d^2}\ \right)^2$$

holds whenever $B = c^2 + 2A\sqrt{A^2+d^2}$. Setting $d = 2ab$ makes $\sqrt{A^2+d^2} = a^2 + b^2$ and so $c^2 = B - 2A\sqrt{A^2+d^2} = 4a^2t^2$ where $t^2 = 5b^2 - a^2$. The latter has complete solution

$$t = h^2 + 5k^2 + 10hk\ , \quad b = h^2 + 5k^2 + 2hk\ , \quad a = 10k^2 - 2h^2$$

which can be obtained from a general solution due to Desboves in 1884 (see [**10**], page 432). After removing their common factors we have the integer edges

$$\begin{aligned} x &= hk(h-k)(h+k)(h-5k)(h+5k)(h+3k)(3h+5k) \\ y &= (h-k)(h+3k)(h-5k)(3k+5k)(h^2+2hk+5k^2)(h^2+10hk+5k^2) \\ z &= 4(5k^2-h^2)(h^2+2hk+5k^2)^2(h^2+10hk+5k^2) \end{aligned}$$

and with the rational substitution $t = h/k$ we obtain the rational parametric system stated above. A search with $k = 1, 2, 3, \cdots$ and relatively prime integers h and k such that $\alpha k < h < \beta k$ where $\alpha = (\sqrt{40}-5)/3$ and $\beta = \sqrt{5}$ found no perfect cuboids for $k \leq 700,000$; these restrictions on h guarantee that no two primitive HK cuboids generated will be the same. The body duals (xy, xz, yz) were also checked.

Around $k = 700,000$ a typical primitive HK cuboid has about 50 decimal digits in each edge, so that the square of its body diagonal has about 100 digits. Now the chance that a 100-digit integer is a perfect square is roughly one in 10^{50}. I am told that our planet earth is composed of about 10^{50} atoms, so it would seem highly unlikely that one could find that single atom somewhere in the earth that represents a perfect square. On the other hand, just because my computer did not found a perfect cuboid does not mean it is not there. More discriminating search methods — somehow exploiting the algebraic structure of the body diagonal — might have a better chance. (See Section 14.) If you want to find a needle in a haystack, first get a really strong magnet . . .

EF Face Cuboids

Euler's quartic identity will also give parametric formulas for face cuboids: we find

$$\begin{aligned} x &= ef(e+2f)(2e+f)(e^2+2ef+3f^2)(3e^2+2ef+f^2) \\ y &= 4ef(e-f)(e+f)(e+2f)(2e+f)(e^2+ef+f^2) \\ z &= 2(e-f)^2(e+f)^2(e^2+4ef+f^2)(e^2+ef+f^2) \end{aligned}$$

and DERIVE verifies that $\sqrt{x^2+y^2}$, $\sqrt{y^2+z^2}$, and $\sqrt{x^2+y^2+z^2}$ are always integers, so that (x,y,z) is indeed a face cuboid. This seems to be the only known parametric system which will generate face cuboids. In [**24**] Allan MacLeod gave a parametric system for edge cuboids; like Bremner [**3**] he used elliptic curve methods.

My computers tested all $|f| < e \leq 300,000$ with $\gcd(e,f) = 1$ and the bad face diagonal was never an integer; the other four face cuboids in each pentad were also tested; none were perfect.

6. Nearly Perfect HK Cuboids

Some authors (for example, [**24**]) have used "nearly perfect" to label cuboids with only one irrational edge or diagonal. However, it seems to me that a nearly perfect cuboid ought to be one in which the irrational feature, whether an edge or a diagonal, is extremely close to an integer. One can construct HK cuboids with body diagonals arbitrarily close to an integer as follows: if we write $x = pr = (a^2-b^2)(c^2-d^2)$, $y = ps = 2cd(a^2-b^2)$, $z = qs = 4abcd$ and recall that $c = 2at$, $d = 2ab$, $t^2 = 5b^2 - a^2$ so that

$$x = (a^2-b^2)(t^2-b^2)\ , \quad y = 2bt(a^2-b^2)\ , \quad z = 4ab^2t\ .$$

Thus when $t = 1$ we have $x^2+y^2+z^2 = A^2+B^2$ where $A = (a^2-b^2)(1+b^2)$ and $B = 4ab^2$. Since $5b^2 - a^2 = t^2 = 1$ we have $x^2+y^2+z^2 = A^2+B^2 = C^2+D$ where $C = 4b^4+5b^2+1$ and $D = -16b^4 - 20b^2$. The Taylor series

$$\sqrt{1+u} = 1 + \frac{1}{2}u - \frac{1}{2\cdot 4}u^2 + \frac{1\cdot 3}{2\cdot 4\cdot 6}u^3 - \cdots$$

gives $\sqrt{x^2+y^2+z^2} \;=\; \sqrt{C^2+D} \;=\; C\sqrt{1+D/C^2}$

$$= \; C + \frac{D}{2C} - \frac{D^2}{8C^3} + \frac{D^3}{16C^5} - \cdots \; = \; (C-2) + O(1/b^4)$$

since $D/2C = -2 + O(1/b^4)$ and $D^2/8C^3 = O(1/b^4)$. Thus the integer nearest the body diagonal is actually $C - 2$ and, when b is large, the fractional part $O(1/b^4)$ is extremely small, as claimed. The equation $a^2 - 5b^2 = -1$ is a special case of Pell's equation and its solutions are well known: take $p_0 = 2$, $q_0 = 1$, $p_1 = q_1 = 4$, $p_{k+1} = 4p_k + p_{k-1}$, and $q_{k+1} = 4q_k + q_{k-1}$ for $k = 1, 2, 3, \cdots$. Then $(a,b) = (p_k, q_k)$ is a solution to $a^2 - 5b^2 = -1$ for each even positive integer k, and these solutions quickly get very large: for $k = 500$ the primitive HK cuboid (x,y,z) has edges with 1260, 945, and 945 digits respectively, and its body diagonal has 627 zeros following the decimal point. This modification of the HK Algorithm will produce primitive rational cuboids with body diagonals having any desired number of zeros following the decimal point; the practical limit depends on the software and the computer's memory. Unfortunately the fractional part of the body diagonals produced by this method will never be exactly zero, so no HK cuboid generated in this fashion can be truly perfect.

7. Euler Cuboids and Lagrange Duals

I mentioned in Section 12 that Andrew Bremner [**3**] found five parametric systems for body cuboids in 1988. Like my 2004 system, Bremner's formulas for the edges are all of degree eight with two integer parameters. Bremner remarked that he had also found systems of degree ten and higher. There is only one known parametric system of degree six; it was discovered independently in the 1700's by Nicholas Saunderson in England and Leonhard Euler in Switzerland (see Dickson [**10**], Chapter XIX). The edges are

$$\begin{aligned} x &= 8mn(m^4-n^4) \;=\; 4abc \\ y &= 2mn(3m^2-n^2)(3n^2-m^2) \;=\; a(c^2-4b^2) \\ z &= (m^2-n^2)(m^2+4mn+n^2)(m^2-4mn+n^2) \;=\; b(c^2-4a^2) \end{aligned}$$

where $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$. The square of the body diagonal is

$$\begin{aligned} x^2+y^2+z^2 &= m^{12}+70m^{10}n^2+15m^8n^4-108m^6n^6+15m^4n^8+70m^2n^{10}+n^{12} \\ &= (m^2+n^2)^2(m^8+68m^6n^2-122m^4n^4+68m^2n^6+n^8) \\ &= (m^2+n^2)^2(a^4+18a^2b^2+b^4)\ . \end{aligned}$$

Historically Saunderson-Euler cuboids have usually been called "Euler cuboids" or "Euler triples" since Euler's fame in continental Europe overshadowed Saunderson's. In 1914 H. C. Pocklington [**25**] proved that $a^4+18a^2b^2+b^4$ is never a perfect square for any $a, b \geq 1$ and hence no Saunderson–Euler cuboid (x, y, z) can be perfect. In 1977 E. Z. Chein [**5**] proved that the body dual (yz, xz, xy) also cannot be perfect. In the case of eighth-degree formulas, the square of the body diagonal is a 16th degree polynomial in two variables, and there seems to be no known method for proving that such polynomials cannot be perfect squares.

In 1983 Jean Lagrange [**17**] published some new results on the family of equations

$$(\star) \qquad x_1^2+y_1^2 = x_2^2+y_2^2 = \cdots = x_n^2+y_n^2 = x_1^2+x_2^2+\cdots+x_n^2$$

where $n \geq 3$ and $x_i \neq x_j$ for $i \neq j$. When $n = 3$ we have

$$x_1^2+x_2^2 = y_3^2\ , \quad x_1^2+x_3^2 = y_2^2\ , \quad x_2^2+x_3^2 = y_1^2$$

so that $(\star)$ generalizes body cuboids. Lagrange proved that if (x_i, y_i) is a solution to $(\star)$ then so is (X_i, Y_i) where

$$(\star\star) \qquad X_i = (n-2)Sx_i - Py_i\ , \quad Y_i = Px_i + (n-2)Sy_i$$

with $S = x_1^2 + \cdots + x_n^2$ and $P = 2(x_1y_1 + \cdots + x_ny_n)$.

Since we are only interested in the case $n = 3$ we can simplify Lagrange's proof: set

$$X_i = ASx_i - By_i \ , \quad Y_i = BPx_i + ASy_i$$

and note that $y_1^2 + y_2^2 + y_3^2 = 2S$. Then for $i = 1, 2, 3$ we have $X_i^2 + Y_i^2 = (A^2S^2 + B^2P^2)S$ and $X_1^2 + X_2^2 + X_3^2 = (A^2S^2 + 2B^2P^2 - ABP^2)S$; equating these and simplifying yields $A = B$; since (X_1, X_2, X_3) will always be reduced to a primitive cuboid, we may assume that $A \perp B$. Hence $A = B = 1$ and this proves $(\star\star)$ for $n = 3$. It is easy to check that

$$X_1^2 + X_2^2 = Y_3^2 \ , \quad X_1^2 + X_3^2 = Y_2^2 \ , \quad X_2^2 + X_3^2 = Y_1^2$$

so that (X_1, X_2, X_3) is indeed a body cuboid. Naturally we call (X_1, X_2, X_3) the *Lagrange dual* of (x_1, x_2, x_3).

To justify this sobriquet we compute the second dual: for $i = 1, 2, 3$ let $\mathcal{X}_i = \mathcal{S}X_i - \mathcal{P}Y_i$ and $\mathcal{Y}_i = \mathcal{P}X_i + \mathcal{S}Y_i$ where $\mathcal{S} = X_1^2 + X_2^2 + X_3^2$ and $\mathcal{P} = 2(X_1Y_1 + X_2Y_2 + X_3Y_3)$. Then $\mathcal{S} = S(S^2 + P^2)$ and $\mathcal{P} = -P(S^2 + P^2)$ and a little matrix algebra gives

$$\begin{bmatrix} \mathcal{X}_i \\ \mathcal{Y}_i \end{bmatrix} = \begin{bmatrix} \mathcal{S} & -\mathcal{P} \\ \mathcal{P} & \mathcal{S} \end{bmatrix} \begin{bmatrix} S & -P \\ P & S \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} = (S^2 + P^2)^2 \begin{bmatrix} x_i \\ y_i \end{bmatrix}$$

which means that $(\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ is just the cuboid (x_1, x_2, x_3) with each edge multiplied by $(S^2 + P^2)^2$. When both are made primitive, they reduce to the same body cuboid.

The Lagrange dual of the body cuboid $(240, 252, 275)$ is the primitive cuboid

$$(-159576240, -152780292, -138830725)$$

and this is much larger than the ordinary dual $(1008, 1100, 1155)$. A surprise is that the Lagrange dual of $(44, 117, 240)$ is the trivial cuboid $(-4, -3, 0)$. The reason for this is that $(44, 117, 240)$ is an Euler cuboid: it is easy to show that when $a^2 + b^2 = c^2$ the Lagrange dual of $(a, b, 0)$ is the Euler cuboid $(-4abc, a(c^2 - 4b^2), b(c^2 - 4a^2))$. Another surprise is that merely changing the edge signs makes the Lagrange duals prolificate: that is, any body cuboid will produce infinitely many different body cuboids. Let $L_0(x_1, x_2, x_3)$ be the Lagrange dual of (x_1, x_2, x_3) and define $L_1(x_1, x_2, x_3) = L_0(-x_1, x_2, x_3)$, $L_2(x_1, x_2, x_3) = L_0(x_1, -x_2, x_3)$, and $L_3(x_1, x_2, x_3) = L_0(x_1, x_2, -x_3)$. Here "=" means that all cuboids are always reduced to primitives. Regarding the L_i for $i = 0, 1, 2, 3$ as operators on the family of all body cuboids, we may compose them at will: for example,

$$L_1L_2(240, 252, 275) = (1601513881200, -3741823994172, 508510959395)$$

while $L_3L_1L_2(240, 252, 275)$ has 38 digits in each edge. One can show that $L_i^{-1} = L_0L_iL_0$ so that operator composition has a nice group structure, and inverses are easily computed.

Negative edges introduce certain delicate complications. Let

$$\begin{array}{ll} I_0(x_1, x_2, x_3) = (x_1, x_2, x_3) & I_1(x_1, x_2, x_3) = (-x_1, x_2, x_3) \\ I_2(x_1, x_2, x_3) = (x_1, -x_2, x_3) & I_3(x_1, x_2, x_3) = (x_1, x_2, -x_3) \end{array}$$

denote the four "identity" operators. It is obvious that $L_0I_i = L_i$, $L_iI_i = L_0$, and $L_0L_i = L_0L_0I_i = I_i$ for $i = 0, 1, 2, 3$. Also $L_1I_2 = L_2I_1 = -L_3$, $L_1I_3 = L_3I_1 = -L_2$, and $L_2I_3 = L_3I_2 = -I_1$. Note that L_1, L_2, and L_3 map trivial cuboids to trivial cuboids.

Finally, we may compose the operators L_0, L_1, L_2, L_3 with the ordinary dual operator $D(x_1, x_2, x_3) = (x_2x_3, x_1x_3, x_1x_2)$. Since $D(a, b, 0) = (1, 0, 0)$ trivial cuboids should be avoided: in particular DL_0 maps any Euler cuboid to $(1, 0, 0)$.

Lagrange-Euler Cuboids and Some Computational Results

The foregoing suggests a new way of computing body cuboids in vast abundance. Given m and n with the usual restrictions $0 < n < m$, $n \perp m$, and $n - m$ odd, we generate the primitive Pythogorean triangle $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$ which in turn generates the Euler cuboid $(4abc, a(c^2 - 4b^2), b(c^2 - 4a^2))$. Of course we know that no Euler cuboid is perfect, nor is the dual of an Euler cuboid, but we can apply the operators

$$L_i \ , \ \ DL_i \ , \ \ L_iD \ , \ \ DL_iD \ , \ \ L_iL_j \ , \ \ DL_iL_j \ , \ \ L_iL_jD \ , \ \ DL_iL_jD \ , \ \ L_iDL_j \ , \ \ \cdots$$

(avoiding compositions which produce repetitions or trivial cuboids) and construct body cuboids at the rate of several million per hour per computer. Since no one has proved that these cannot be perfect, who knows what the computers might find?

The "Slow" Program: This program transformed each Euler cuboid produced by suitable (m, n) into 166 different Lagrange-Euler cuboids; the largest were manufactured by operators of the form $L_iL_jL_k$ and these cuboids typically had several hundred digits in each edge, though never more than a thousand. Repeated cuboids were avoided as much as possible; the basic Euler cuboids generated by (m, n) were certainly all different; the total number of cuboids produced was asymptotic to $0.3367m^2$ (the exact counts for $m \leq 1000$ and $m \leq 2000$ were 33,674,926 and 134,651,730 respectively). A curious nearly perfect cuboid was found in the first few minutes of the computation: $(m, n) = (326, 13)$ transformed by DL_1L_3 produce a cuboid with a body diagonal consisting of 183 digits followed by $.0000000001955\cdots$ (nine zeros).

The "Fast" Program: Each Euler cuboid was transformed into only 14 different cuboids, whose edges rarely exceed 120 digits. This program ran about fifty times faster than the "slow" program; the number of cuboids tested was asymptotic to $0.02837m^2$. Still another remarkable nearly perfect cuboid appeared rather early: the Euler cuboid generated by $(m, n) = (20364, 5561)$ and transformed by DL_1D had a body diagonal with 99 digits followed by $.000000000004371\cdots$ (eleven zeros).

Lagrange-Butler Cuboids

Since $L_0L_0 = I_0$ it is obvious that a body cuboid C is an Euler cuboid if L_0C is a trivial cuboid; this gives a simple way of identifying Euler cuboids. For example, only 92 of the 10,932 Butler cuboids (the primitive body cuboids with all edges less than 10^{10} — see Section 1) are Euler cuboids; this is less than one percent. The "slow" program was applied to all the Butler cuboids and, as one would expect, there were numerous repetitions as well as over 4500 trivial cuboids. The most nearly perfect of all the primitive nontrivial cuboids produced had a body diagonal with 32 digits followed by $.00000001018\cdots$ (seven zeros). See Section 3.

The "slow" program was also applied to the 26,546 primitive body cuboids described in Section 9; only 170 of these were Euler cuboids, again less than one percent; all 170 were of Type 1 or 3. There were also numerous repetitions among the 4,395,348 body cuboids produced; 11,288 of these were trivial. The most nearly perfect was the same as the one produced by the Butler cuboids.

8. Ivan Korec Methods

In 1992 Korec [**15**] reported that the body diagonal of a perfect cuboid must exceed eight billion. He used PASCAL, a software not designed for high–precision integers, and so he had to rely on a variety of ingenious congruence tricks, which pervade much of his paper. Since UBASIC handles large numbers so easily, we will not be concerned here with Korec's congruences. Moreover, Korec's description of his computer program was rather sketchy, so I prefer to describe my own UBASIC program, which of course is based on Korec's fundamental ideas. In 2006 my computers used this program to raise Korec's lower bound from eight billion to 120 billion.

Suppose that a primitive perfect cuboid does exist, with edges (x_1, x_2, x_3) and face diagonals

$$y_1 = \sqrt{x_2^2 + x_3^2}\ , \quad y_2 = \sqrt{x_1^2 + x_3^2}\ , \quad y_3 = \sqrt{x_1^2 + x_2^2}\ .$$

Then its body diagonal z satisfies $z^2 = x_1^2 + x_2^2 + x_3^2 = x_1^2 + y_1^2 = x_2^2 + y_2^2 = x_3^2 + y_3^2$ and we have the following elementary

> **Facts.** One edge, say x_3, must be odd; the body diagonal z is odd, and the edges x_1 and x_2 are divisible by four; the face diagonals y_1 and y_2 are odd, and the other face diagonal y_3 is divisible by four.

Proof Certainly all three edges cannot be even (since the cuboid is primitive) and so we may assume the edge x_3 is odd. Suppose x_1 is also odd; then y_2 would be even, which gives the contradiction $0 \equiv y_2^2 = x_1^2 + x_3^2 \equiv 1 + 1 \bmod 4$ and so x_1 must be even. Similarly x_2 is even, so that y_1, y_2, x_3, and z are all odd. Next suppose $x_1 = 4a + 2$; now the square of any odd number is equal to one modulo eight, so that $1 \equiv y_2^2 = x_1^2 + x_3^2 \equiv 4 + 1 \bmod 8$ and this contradiction gives $4|x_1$. Similarly $4|x_2$ and the remaining statements are now obvious. **Qed**

The next result is crucial for our computer search; it was apparently new in 1992, but its proof requires only undergraduate number theory.

Fact If p is a prime divisor of the body diagonal z then $p \equiv 1 \bmod 4$.

Proof Suppose $p \equiv 3 \bmod 4$ is a prime divisor of z; then $x_1^2 + y_1^2 = z^2 \equiv 0 \bmod p$. We claim that p must divide x_1. Suppose not: then p and x_1 are relatively prime, so there are integers a and b such that $ax_1 + bp = 1$; then $ax_1 \equiv 1 \bmod p$ and so $a \equiv x_1^{-1} \bmod p$. By elementary properties of the Legendre symbol we have

$$(-1/p) = (-1)^{(p-1)/2} = (-1)^{2k+1} = -1$$

since $p = 4k + 3$; thus -1 is a quadratic nonresidue modulo p. But by our assumption

$$(x_1^{-1} y_1)^2 + 1 = x_1^{-2}(y_1^2 + x_1^2) \equiv x_1^{-2} \cdot 0 = 0 \bmod p$$

and hence $(x_1^{-1} y_1)^2 \equiv -1 \bmod p$, which means that -1 is a quadratic residue modulo p; this contradiction shows that p divides x_1. Similarly p divides x_2 and x_3 contradicting our assumption that the cuboid is primitive. **Qed**

A trivial but important corollary is that $z \equiv 1 \bmod 4$.

Girard's Theorem and Sums of Two Squares

Albert Girard (1596-1633) was apparently the first person (see **[10]**, Chapter VI) to observe that primes of the form $p = 4k + 1$ could be expressed as the sum of two squares in essentially only one way, as the examples $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$ suggest. Primes of the form $p = 4k + 3$ have no such representations; indeed, such primes cannot even be expressed as the sum of two *rational* squares. Fermat claimed to have an "irrefutable proof" of Girard's Theorem, as it came to be called, but the first accepted proof was given by Euler a century later, and it cost him considerable effort. Fermat called Girard's Theorem "the fundamental theorem on right triangles" since for each Girard prime $p = 4k + 1$ there is essentially only one right triangle with integer legs and hypotenuse p. The elementary identity

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$$

shows that $65 = 5 \cdot 13 = (2^2 + 1^2)(2^2 + 3^2) = 8^2 + 1^2 = 4^2 + 7^2$ has two representations as the sum of two squares; let us call these *Girard representations.*

Given any product z of Girard primes, our objective is to compute all possible Girard representations of z^2. For example $z = 65 = 5 \cdot 13$ is a typical candidate and a short computer search finds just four Girard representations:

$$65^2 = 16^2 + 63^2 = 52^2 + 39^2 = 56^2 + 33^2 = 60^2 + 25^2 \,.$$

In any Girard representation of z^2 one number is always odd and the other is always divisible by four; the proof is a simple modulo eight argument. The four representations when z has two different prime factors are

$$\begin{aligned}(a^2 + b^2)^2(c^2 + d^2)^2 &= [2ab(c^2 + d^2)]^2 + [(a^2 - b^2)(c^2 + d^2)]^2\\ &= [2cd(a^2 + b^2)]^2 + [(c^2 - d^2)(a^2 + b^2)]^2\\ &= [2(ac + bd)(ad - bc)]^2 + [(a^2 - b^2)(c^2 - d^2) + 4abcd]^2\\ &= [2(ac - bd)(ad + bc)]^2 + [(a^2 - b^2)(c^2 - d^2) - 4abcd]^2\end{aligned}$$

and this is merely the tip of an infinite iceberg. Indeed if z has 2, 3, 4, 5, 6, 7, $\cdots$ distinct Girard prime factors then z^2 has respectively 4, 13, 40, 121, 364, 1093, $\cdots$ Girard representations. The recursion rule is to multiply by three and then add one. An equivalent formula: if z has n different prime factors then z^2 has $(3^n - 1)/2$ Girard representations. When $z = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ we have exactly $[(2e_1 + 1)(2e_2 + 1) \cdots (2e_k + 1) - 1]/2$ Girard representations. In particular if $z = p^n$, then z^2 has only $[(2n + 1) - 1]/2 = n$ Girard representations. Given $z = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with $e_1 + e_2 + \cdots + e_k = n$ there are $p(n)$ different sets of Girard representations, where $p(n)$ is the partition function, first studied by Euler and later by Hardy, Ramanujan, and many others.

Why are we interested in computing all these representations, and what do they have to do with the search for a perfect cuboid? **Here is the reason:** Let z be any product of Girard primes; suppose we can find three different Girard representations

$$z^2 = a_1^2 + b_1^2 = a_2^2 + b_2^2 = a_3^2 + b_3^2$$

where the a_i are odd, the b_i are divisible by four, and $b_1^2+b_2^2=b_3^2$. Then

$$\begin{aligned} a_3^2+b_1^2 &= z^2-b_3^2+b_1^2 = z^2-b_2^2 = a_2^2 \\ a_3^2+b_2^2 &= z^2-b_3^2+b_2^2 = z^2-b_1^2 = a_1^2 \\ a_3^2+b_1^2+b_2^2 &= a_3^2+b_3^2 = z^2 \end{aligned}$$

and consequently (a_3,b_1,b_2) is a **perfect cuboid** with body diagonal z and face diagonals a_1, a_2, b_3. On the other hand, if $\{a_i^2+b_i^2\}$ is the set of all possible Girard representations of z^2 and if $b_i^2+b_j^2 \neq b_k^2$ for all i,j,k then z cannot be the body diagonal of a perfect cuboid, and the computer will proceed to test the next integer greater than z that is a product of Girard primes.

The Recursion Algorithm

Given $z=p_1p_2\cdots p_n$ where the p_i are Girard primes, not necessarily distinct, first compute the unique positive integers a_i (even) and b_i (odd) such that $p_i=a_i^2+b_i^2$. Set $q_i=2a_ib_i$, $r_i=a_i^2-b_i^2$, and $M_i=p_1\cdots p_i$ so that each r_i is odd, each q_i is divisible by four, and $p_i^2=q_i^2+r_i^2$. The core of my UBASIC program is the following subroutine:

```
X(1)=2*A(1)*B(1):M=P(1):M2=M∧2:C=1:D=1
for L=2 to N:Q=2*A(L)*B(L):R=A(L)∧2-B(L)∧2
for I=1 to D:X=X(I):Y=isqrt(M2-X∧2)
inc C:X(C)=Q*Y+R*X:inc C:X(C)=Q*Y-R*X
inc C:X(C)=X*P(L):next I:inc C:X(C)=Q*M
gosub [1]:M=M*P(L):M2=M∧2:next L:return
```

The subroutine at `[1]` sets each `X(I)` equal to its absolute value, removes any repetitions, overwrites these values into `X(I) for I=1 to S`, and sets the counters `C` and `D` equal to `S`. To see why the code works, consider the following:

I. If we set $x=q_1$ and $y=r_1$ then $x^2+y^2=p_1^2=M_1^2$.

II. At the second level (`L=2`) we have:

(1) If $x=q_1p_2$ and $y=r_1p_2$ then $x^2+y^2=M_2^2$.
(2) If $x=q_2M_1$ and $y=r_2M_1$ then $x^2+y^2=M_2^2$.
(3) If $x=r_1q_2\pm r_2q_1$ and $y=r_1r_2\mp q_1q_2$ then

$$x^2+y^2=(r_1^2+q_1^2)(r_2^2+q_2^2)=p_1^2p_2^2=M_2^2\,.$$

III. At the third level (`L=3`) let (x,y) be any of the four Girard representations computed at the second level.

(1) If $X=xp_3$ and $Y=yp_3$ then $X^2+Y^2=M_3^2$.
(2) If $X=q_3M_2$ and $Y=r_3M_2$ then $X^2+Y^2=M_3^2$.
(3) If $X=q_3y\pm r_3x$ and $Y=r_3y\mp q_3x$ then

$$X^2+Y^2=(q_3^2+r_3^2)(x^2+y^2)=p_3^2M_2^2=M_3^2\,.$$

By induction, at the n^{th} level we will have found x and y such that $x^2+y^2 = M_n^2 = z^2$ with only the x-values stored in the memory array `X(I)`. Note that if there are no repetitions (which always happens when the p_i are distinct Girard primes) then at each level the number of Girard representations is one more than three times the number found in the preceding level; this gives the familiar progression 1, 4, 13, 40, 121, 364, 1093, $\cdots$.

This recursion subroutine is fast: it will find a complete set of Girard representations $z^2 = a_i^2 + b_i^2$ for a candidate $z \approx 100$ billion in less than a second. The only bottleneck in the program is the subroutine which checks whether $b_i^2 + b_j^2 = b_k^2$ for some distinct i, j, k; when there are s different Girard representations that check is $O(s^3)$, but $s > 1000$ is a mercifully rare event. When s is large the check also requires a great deal of computer memory: I expect UBASIC to reach its limit when the body diagonal exceeds 150 billion. Perhaps when s gets too large the values $\{b_i^2 : i = 1, \cdots, s\}$ could be stored temporarily in a hard disk file; that's a future bridge to cross.

9. Epilogue: Does a Perfect Cuboid Exist?

No one knows, of course, and it is just this uncertainty that makes the problem so seductive. It is human nature to want to succeed where others have failed. We have a touch of smug pity for the past generations struggling along with their sluggish antique computers, or no computers at all; no doubt future generations will feel the same way about us. At first there is great enthusiasm for each new search algorithm — maybe this is the one that will finally conquer the problem! — but the excitement soon evaporates when no perfect cuboid is found. And then come the excuses: "the Diophantine equations seem to be too restrictive" or "a solution beyond this point seems unlikely" or "there are too many symmetry requirements for the Pythagorean generators." This all reminds me of Aesop's fox and the sour grapes, so I will let these quotes remain anonymous.

On the Internet there are several amateur "proofs" that a perfect cuboid does not exist. Some are quite compelling until you discover the first mistake; others are hopelessly incompetent. One amateur disproves existence in a single paragraph, and then exterminates odd perfect numbers with the same impressive brevity. After conquering the perfect cuboid, another amateur argues that rational numbers are uncountable. Squaring the circle seems to be currently out of fashion. My personal aversion to lawsuits prevents me from divulging names. Type "perfect cuboid" into Google and explore.

Some Statistical Observations

What is the likelihood that a primitive body cuboid is perfect? Let (a, b, c) be a primitive body cuboid and let $N = a^2 + b^2 + c^2$ be the square of its body diagonal; then (a, b, c) is perfect if and only if N is a perfect square. Let m be the integer square root of N; then $m^2 \le N < (m + 1)^2$ and so there are $(m + 1)^2 - m^2 = 2m + 1$ possible values for N within this range. Now many of these can be excluded: since $N \equiv 1 \bmod 8$ (see Section 6) there only $1 + m\backslash 4$ choices for N when m is odd; the backwards virgule \ is integer division. Thus when m is odd the probability that N is a perfect square is $1/(1 + m\backslash 4)$. Note that if m is even then N cannot be a perfect square, and so $p = 0$ in this case.

Think of this process as an infinite game of chance: we win if some body cuboid is perfect and we lose if every body cuboid is not perfect. What is the probability that we win or lose? Let $\{C_i : i = 1, 2, \cdots, I\}$ be any finite sequence of different primitive body cuboids with $C_i = (a_i, b_i, c_i)$ for each i. By the preceding observations, the probability that C_i is a perfect cuboid is $p_i = 1/(1 + m\backslash 4)$ where m is the integer square root of $a_i^2 + b_i^2 + c_i^2$; if m is even then $p_i = 0$. Now $q_i = 1 - p_i$ is the probability that C_i is not perfect, so that the probability that no C_i $(i = 1, 2, \cdots, I)$ is perfect is $Q_I = q_1 q_2 \cdots q_I$ and hence the probability that some C_i is perfect is $P_I = 1 - Q_I$.

Section 9 summarized a hard disk data file containing the 26546 different primitive body cuboids generated by the Pythagorean parameters a, b, c, d with $a \leq 5000$. A simple computer program found the probability that at least one of these body cuboids is perfect to be $P_B = 0.01777$, about one in 56. Similar calculations estimate that the probabilities for face and edge cuboids to be $P_F = 0.01294$ and $P_E = 0.00418$ respectively. (Obviously only real edge cuboids have any chance of being perfect.) Thus we estimate the probability that no cuboid is perfect to be $(1-P_B)(1-P_F)(1-P_E) \approx 0.96547$ and so the probability that a perfect cuboid exists is 0.03453, or about one in 29.

Statistics and Number Theory

One must be wary of statistics in number theory. We may argue that there is one chance in 29 that a perfect cuboid exists, but in fact the creature either exists or it doesn't: that is, the true probability is either one or zero, and nothing in between. Consider for example the Diophantine equation $a^3 + b^3 = c^3$; assuming that the values $a^3 + b^3$ are randomly distributed, one can argue that $a^3 + b^3 = c^3$ has better than a ninety percent chance of having a solution with $a, b \leq 10000$. But this is nonsense! By Fermat's Last Theorem, there is no solution and so the correct probability is zero. The operative phrase here is "randomly distributed" — evidently something always prevents $a^3 + b^3$ from being a perfect cube, so the distribution is not really random. Similarly we can argue that probability is about 43% that $a^4 + b^4 = c^4$ has a solution with $a, b \leq 10000$, but again Fermat's Last Theorem assures us there is no solution. On the other hand, Euler and many lesser mathematicians believed that $a^4 + b^4 + c^4 = d^4$ had no solution, whereas statistics gives a better than 80% chance that there is a solution with $a, b, c \leq 10^6$; the smallest solution

$$414560^4 + 217519^4 + 95800^4 = 422481^4$$

was discovered in 1988, and thanks to elliptic curve theory, one can generate infinitely many primitive solutions from this single solution. Euler also believed that the sum of four fifth powers could not be a fifth power, but then

$$135^5 + 110^5 + 84^5 + 27^5 = 144^5$$

was found by a computer search in 1966, and is still the only known primitive solution; statistics give only about one chance in six for the existence of a solution. Finally there is $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$ with no known solutions; the odds are only about one in twenty that a solution exists, but that doesn't *prove* anything. For more computational results on sums of like powers, see [**19**]; except for a few isolated results, surprisingly little work as been done on this subject since [**19**] appeared forty years ago, despite the present ubiquity of desktop computers.

Personally the odds (one in 29) do not convince me that a perfect cuboid does not exist. Would you fly on an airplane if you knew it had one chance in 29 of crashing? We know that a perfect cuboid must have some edge greater than 10^{10} and that its body diagonal must be greater than 10^{11}. Yet these lower bounds are really quite small: my computers find primitive body, face, and edge cuboids larger than this every day, and no one knows when Korec's method may strike gold. The computational number theory pioneer D. H. Lehmer (1905–1991) used to say that "Happiness is just around the corner." Until I see a rigorous proof that a perfect cuboid does not exist, I am not turning off my computers. To stop now would just be Sour Grapes.

A Clarion Call for Distributed Computing

Wikipedia defines Distributed Computing as "a method of computer processing in which different parts of a program are run simultaneously on two or more computers that are communicating with each other over a network." Perhaps the two best known mathematical examples of this are the Cunningham Project (which prepares factorization tables for numbers of the form $b^n \pm 1$ where $b = 2, 3, 5, 6, 7, 10, 11, 12$) and GIMPS (the Great Internet Mersenne Prime Search, which seeks new primes of the form $2^p - 1$ where p is prime). For many more similar projects check out distributedcomputing.info on the Internet. The idea is simple: a large computation is broken down into thousands of little pieces, and these are farmed out to thousands of volunteer private and otherwise idle computers scattered all around the world. The search for primitive body, face, and edge cuboids is obviously a splendid candidate for this "divide and conquer" approach. Even if a perfect cuboid were never found, the large data base generated might lead to new insights on this obstinate problem, whose roots go back almost three hundred years. My nine desktop computers (actually they are mostly *under* my desk) took a year to find all 26,546 primitive body cuboids with dominant parameter $a \leq 5000$; since this computation is $O(a^4)$, at this rate it will take another fifteen years before they reach $a = 10000$. One thousand ordinary desktop machines could finish this job in less than a week!

Bibliography

[**1**] Ayoub B. Ayoub: Integral solutions to the equation $x^2 + y^2 + z^2 = u^2$: a geometrical approach, *Mathematics Magazine*, **57** (1984) 222–223.

[**2**] Raymond A. Beauregard & E. R. Suryanarayan: Pythagorean Boxes, *Mathematics Magazine*, **74** (2001) 222–226.

[**3**] Andrew Bremner: The rational cuboid and a quartic surface, *Rocky Mountain Journal of Mathematics*, **18** (1988) 105–121.

[**4**] Bill Butler: The "integer brick" problem (The Euler brick problem). Look up www.durangobill.com.

[**5**] E. Z. Chein: On the derived cuboid of an Eulerian triple, *Canadian Mathematical Bulletin*, **20** (1977) 509–510.

[**6**] Yong–Gao Chen & Shu-Guang Guo: On the rational cuboids with a given face, *Journal of Number Theory* **112** (2005) 205–215.

[**7**] W. J. A. Colman: On certain semi-perfect cuboids, *Fibonacci Quarterly*, **26** (1988) 54–57.

[8] W. J. A. Colman: Some observations on the classical cuboid and its parameter solutions, *Fibonacci Quarterly*, **26** (1988) 338–343.

[9] W. J. A. Colman: A perfect cuboid in Gaussian integers, *Fibonacci Quarterly*, **32** (1994) 266–268.

[10] Leonard Eugene Dickson: *History of the Theory of Numbers*, Volume II.

[11] Leonhard Euler: *Elements of Algebra* (Fifth Edition, 1840) 443–447.

[12] Richard K. Guy: *Unsolved Problems in Number Theory* (Second Edition, 1994) 173–181.

[13] Ivan Korec: Nonexistence of a small perfect rational cuboid, I, *Acta Mathematica University Comenian*, **42/43** (1983) 73–86.

[14] Ivan Korec: Nonexistence of a small perfect rational cuboid, II, *Acta Mathematica University Comenian*, **44/45** (1984) 39–48.

[15] Ivan Korec: Lower bounds for perfect rational cuboids, *Mathematica Slovaca*, **42** (1992) 565–582.

[16] Maurice Kraitchik: On certain rational cuboids, *Scripta Mathematica*, **11** (1945) 317–326.

[17] Jean Lagrange: Sets of n squares of which any $n-1$ have their sum square, *Mathematics of Computation*, **41** (1983) 675–681.

[18] M. Lal & W. J. Blundon: Solutions of the Diophantine equations $x^2 + y^2 = l^2$, $y^2 + z^2 = m^2$, $z^2 + x^2 = n^2$, *Mathematics of Computation*, **20** (1966) 144–177.

[19] L. J. Lander, T. R. Parkin, & J. L. Selfridge: A survey of equal sums of like powers, *Mathematics of Computation*, **21** (1967) 336–459.

[20] John Leech: The rational cuboid revisited, *American Mathematical Monthly*, **84** (1977) 518–533.

[21] John Leech: Five tables related to rational cuboids, *Mathematics of Computation*, **32** (1978) 657–659.

[22] John Leech: A remark on rational cuboids, *Canadian Mathematics Bulletin*, **24(3)** (1981) 377–378.

[23] Florian Luca: Perfect cuboids and perfect square triangles, *Mathematics Magazine*, **73** (2000) 400–401.

[24] Allan J. MacLeod: Parametric expressions for a "nearly-perfect" cuboid. PCTex document at http://maths.paisley.ac.uk.

[25] H. C. Pocklington: Some diophantine impossibilities, *Proceedings of the Cambridge Philosophical Society*, **17** (1914) 110–121.

[26] Randall L. Rathbun: (1) Table of equal area Pythagorean triangles, form coprime sets of integer generator pairs. (2) The integer cuboid table, with body, edge, and face type of solutions + The integer cuboid auxiliary table (with Torbjörn Granlund). (3) The classical rational cuboid table of Maurice Kraitchik (also with Granlund). Reviewed in *Mathematics of Computation*, **62** (1994) 440–443.

[27] Randall L. Rathbun: Computer searches for the perfect integer cuboid (1999). Article and report at www.math.niu.edu.

[28] W. G. Spohn: On the integral cuboid, *American Mathematical Monthly*, **79** (1972) 57–59.

[29] W. G. Spohn: On the derived cuboid, *Canadian Mathematical Bulletin*, **17** (1974) 575–577.