

Sums of cubes: algorithmic and numerical aspects

François Hennecart

A2X, Université Bordeaux 1

January 13, 1997

[summary by Alain Plagne]

Abstract

Here are presented results of joint work by J.-M. Deshouillers, F. Hennecart and B. Landreau on sums of powers (and especially of three and four cubes): do they have a positive density? is their behaviour that of the probabilistic model? Moreover, they exhibit a candidate for being the largest integer which is not sum of four cubes, namely 7 373 170 279 850.

1. Sums of cubes

In 1770, Waring wrote that every integer is the sum of 4 squares, 9 cubes, 19 biquadrates and so on, meaning that for each integer k , there exists a constant $g(k)$ such that every integer N is the sum of at most $g(k)$ k -th powers. It was not until 1909, that Hilbert [11] proved it, by a difficult argument.

We say that an integer is C_k if it is the sum of at most k cubes. In 1912, Kempner and Wierferich proved that every integer is C_9 , that is sum of at most 9 cubes. In 1939, Dickson [7] proved that, except 23 and 239, every integer is C_8 . Later, Linnik [15] (and later Watson [21] and Mac Curley [16]), proved that every sufficiently large integer is C_7 . Papers by Bohman and Fröberg [2] and Romani [17] suggest that there are only 15 integers C_8 and not C_7 (the largest one being 454), 121 that are C_7 and not C_6 (the largest one being 8042), and 3922 that are C_6 and not C_5 (the largest one being 1290740).

The circle method, introduced and developed by Hardy, Littlewood and Ramanujan [10] yields an asymptotic formula for the number of solutions to some Diophantine equations. It gives, for large enough s ,

$$(1) \quad \mathcal{R}_s(N) = |\{0 \leq x_1, \dots, x_s \leq N, N = x_1^3 + \dots + x_s^3\}| \sim \mathcal{S}_s(N) \frac{\Gamma(4/3)^s}{\Gamma(s/3)} N^{s/3-1}$$

when N tends to $+\infty$. The factor $\mathcal{S}_s(N)$ is commonly called the singular series

$$\mathcal{S}_s(N) = \sum_{q=1}^{\infty} \sum_{\substack{a \bmod q \\ (a,q)=1}} q^{-s} S(a, q)^s e_q(-aN),$$

where $e_q(u) = \exp(2\pi i u/q)$ and

$$S(a, q) = \sum_{m=1}^q e_q(am^k).$$

This singular series reflects the arithmetic properties of sums of cubes and usually does not imply difficulty because (when it is convergent) it can be written as an Eulerian product (that is a

product over primes). In 1985, Vaughan [19] proved that (1) holds true for $s \geq 8$ and two years later, showed [20] the lower bound

$$\mathcal{R}_7(N) \gg \mathcal{S}_7(N)N^{4/3}.$$

The usual conjecture is that (1) is true as soon as $s \geq 4$. In this direction, Davenport [4] proved, in 1939, that

$$E(N) = |\{n \leq N, \text{ such that } n \text{ is not } C_4\}| \ll_\epsilon N^{\frac{29}{30}+\epsilon},$$

which implies that almost every integer is C_4 . Recently the exponent has been reduced to $37/43$ [3].

We denote by $\mathcal{R}'_3(n)$ the number of solutions of $x^3 + y^3 + z^3 = n$, with $0 \leq x \leq y \leq z$. It is clear that the number $f_3(N)$ of integers $n \leq N$ which are sums of three positive cubes (that is such that $\mathcal{R}'_3(n) > 0$) cannot exceed the number of triples (x, y, z) subject to $x^3 + y^3 + z^3 \leq N$ and $0 \leq x \leq y \leq z$, asymptotically equal to

$$\frac{1}{6}\Gamma(4/3)^3 N = 0.1186\dots N.$$

Now, a natural question is: does the set of sums of 3 cubes have a density? If so, is it strictly positive? Barrucand [1] computed $f_3(x)$ for $1 \leq x \leq 288000$ and conjectured that it was $o(x)$, as x tends to ∞ . Vaughan [18] proved in the opposite direction that $f_3(x) \gg_\epsilon x^{8/9-\epsilon}$, improved to $f_3(x) \gg_\epsilon x^{19/21-\epsilon}$ in [19] and then to $f_3(x) \gg_\epsilon x^{11/12-\epsilon}$ in [20] and Hooley [12] conjectured, contrarily to Barrucand, that $f_3(x) \asymp x$. Hooley's approach consists in studying

$$M(x) = \sum_{n \leq x} \mathcal{R}_3(n)^2.$$

He proves a first lower bound

$$M(x) \geq 36 \sum_{n \leq x} \mathcal{R}'_3(n) \sim 6\Gamma(4/3)^3 x,$$

which corresponds to the so-called ‘‘combinatorial’’ contribution, and then a second, taking now into account the ‘‘arithmetic’’ contribution: if

$$F(\theta) = \sum_{n \leq x} \mathcal{R}_3(n)e(n\theta),$$

we have (by just considering the contribution of major arcs)

$$M(x) \geq \int_0^1 |F(\theta)|^2 d\theta \geq \Gamma(4/3)^6 \mathcal{S}x + o(x),$$

with

$$(2) \quad \mathcal{S} = \sum_{q=1}^{\infty} \sum_{\substack{a \bmod q \\ (a,q)=1}} |S(a,q)/q|^6.$$

Hooley conjectures that these two contributions are ‘‘independent’’ and thus that their sum gives the good equivalent for $M(x)$, namely

$$(3) \quad M(x) \sim (6\Gamma(4/3)^3 + \Gamma(4/3)^6 \mathcal{S})x,$$

which would imply by Cauchy inequality that sums of 3 cubes have a lower density.

2. The first probabilistic approach for sums of three cubes

This is due to Erdős and Rényi [8] in 1960. They consider a sequence $(\xi_n)_{n \geq 1}$ of Bernoulli independent random variables such that

$$\Pr(\xi_n = 1) = \alpha_n = \frac{1}{3n^{2/3}}.$$

The random variable counting the number of representations of N as the sum of 3 pseudo-cubes (that is integers n for which $\xi_n = 1$) is

$$R_3(N) = \sum_{\substack{N=h_1+h_2+h_3 \\ h_1 < h_2 < h_3}} \xi_{h_1} \xi_{h_2} \xi_{h_3}.$$

Erdős and Rényi announced that $R_3(N)$ follows asymptotically a Poisson law:

$$\Pr(R_3(N) = r) \xrightarrow{N \rightarrow +\infty} \frac{\gamma^r}{r!} e^{-\gamma},$$

where $\gamma = \Gamma(4/3)^3/6$. But their “proof” contained a gap that Landreau [14] recently filled in a general context (cf. [9]) by using original correlation inequalities which also enable him to show that the density of sums of 3 pseudo-cubes is almost surely $1 - e^{-\gamma} = 0.1119\dots$. This model has the disadvantage to give a positive density for the sums of 2 pseudo-squares, although sums of 2 squares are known to have zero density [13].

3. Second probabilistic approach. Sums of three cubes continued

The previous paradox came at least from the following fact: the model did not deal with arithmetic properties of sums of powers. A new model has been recently presented [6] taking into account arithmetic parameters.

Let $K \geq 1$. One builds an integer random sequence $(\mu_l^{(k)})_{l \geq 1}$ restricted to be equal to k^3 modulo K and satisfying

$$\mu_l^{(k)} \sim (k + lK)^3$$

almost surely.

Let us denote

$$\rho_3(k, K) = |\{(k_1, k_2, k_3), 1 \leq k_i \leq K : k = k_1^3 + k_2^3 + k_3^3 \pmod{K}\}|$$

and

$$R'_3(n, K) = |\{n = \mu_{l_1}^{(k_1)} + \mu_{l_2}^{(k_2)} + \mu_{l_3}^{(k_3)}, \mu_{l_1}^{(k_1)} < \mu_{l_2}^{(k_2)} < \mu_{l_3}^{(k_3)}, n = k_1^3 + k_2^3 + k_3^3 \pmod{K}\}|.$$

Once again, it has been shown that $R'_3(n, K)$ converges in distribution towards a Poisson law:

$$\Pr\{R'_3(n, K) = r\} \xrightarrow[n=k \pmod{K}]{n \rightarrow \infty} \frac{1}{r!} \lambda(k, K)^r e^{-\lambda(k, K)},$$

with

$$\lambda(k, K) = \gamma \frac{\rho(k, K)}{K^2}.$$

We can show also that the density of integers such that $R'_3(n, K) > 0$ is almost surely $1 - \delta_0(K)$ where

$$\delta_0(K) = \frac{1}{K} \sum_{k=1}^K e^{-\lambda(k, K)}.$$

Notice that it is satisfactory to observe that the probabilistic square mean value satisfies

$$\frac{1}{x} \sum_{n \leq x} R'_3(n, K)^2 \sim \Gamma(4/3)^3 + \Gamma(4/3)^6 \mathcal{S}'_2(K)/6$$

which is consistent with Hooley's conjecture (3) (for the definition of $\mathcal{S}'_2(K)$ see the next section).

4. Numerical viewpoint.

It is now natural to ask what happens when K tends to infinity. It seems reasonable to consider the following multiplicatively increasing sequence of moduli

$$K_B = \prod_{p^\alpha \leq B} p^\alpha.$$

Using convexity of the exponential, we first show that $\delta_0(K_B)$ has a limit δ_0 when B tends to infinity. Then in order to find a good approximation for δ_0 , we compute $\delta_0(K_B)$ for a big value of B , by developing it in series

$$\delta_0(K_B) = \sum_{i=0}^I (-1)^i \frac{\gamma^i}{i!} \mathcal{S}'_i(K_B) + R(K_B),$$

where

$$\mathcal{S}'_i(K_B) = \frac{1}{K_B} \sum_{k \bmod K_B} \left(\frac{\rho(k, K_B)}{K_B^2} \right)^i$$

and

$$|R(K_B)| \leq \frac{\gamma^{I+1}}{(I+1)!} \mathcal{S}'_{I+1}(K_B).$$

The multiplicativity of the $\mathcal{S}'_i(K_B)$ is used to estimate them efficiently. Computations have been done using PARI package. For example, with a B around 5000, the truncation parameter I has to be around 18000. Now we use the inequality

$$0 \leq \delta_0 - \delta_0(K_B) \leq \frac{\gamma^2}{2} (\mathcal{S} - \mathcal{S}'_2(K_B)),$$

where \mathcal{S} , defined by equation (2) appears to be also the limit of $\mathcal{S}'_2(K_B)$ as B tends to infinity. Practically, numbers of the form of K_B are replaced by numbers with the following form

$$\prod_{\substack{p^\alpha < B_1 \\ \alpha \geq 2}} p^\alpha \prod_{\substack{p < B_2 \\ p \equiv 1 \pmod{3}}} p.$$

This finally allows us to deduce

$$0.09992 \leq \delta_0 \leq 0.09997.$$

The previous method did not permit to compute δ_0 with an arbitrary number of significant digits. Ph. Flajolet indicated a more efficient method consisting in the use of the Mellin transform. Using the formula

$$e^{-x} = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} \Gamma(s) \frac{x^{-s}}{s} ds$$

valid for any $c > 1, x > 0$, we get

$$(4) \quad \delta_0(K) = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} \Gamma(s) \mathcal{S}'_{-s}(K) \frac{ds}{s}$$

where

$$\mathcal{S}'_{-s}(K) = \frac{1}{K} \sum_{k \bmod K} \left(\frac{\rho(k, K)}{K^2} \right)^{-s}.$$

It then remains to estimate (4) by numerical integration.

5. About 7 373 170 279 850

As asserted before, one expects that every sufficiently large integer is C_4 . Western's conjectures [22] assert that the size of this "last" non- C_4 integer has to be in the range between 10^{12} and 10^{14} . Practically, it is intractable to test every integer between 10^{12} and 10^{13} for example. But the repartition of cubes in arithmetical progressions is far from being regular: this leads to the idea of discriminating the search depending on the class modulo a good integer. So, the strategy has been the following: try to "find" the last non- C_4 integer N_0 in each class modulo 9. It is considered that it is found if no other non- C_4 integer is found between N_0 and $10N_0$ (10 is a factor seeming largely sufficient in view of previous experiments). This process allowed to treat the cases of every residue class modulo 9, except 4 and 5. For these ones, it has been needed to proceed to a new discrimination (modulo 7). So there were 14 residue classes modulo 63 to examine. This discrimination has allowed to finish all computations. This has permitted to conjecture that the last non- C_4 integer is 7 373 170 279 850; it appears to be equal to 32 modulo 63. Computations have needed 8000 hours. Note that the size of this integer is in accordance with Western's conjectures. This work is more precisely presented in [5].

References

- [1] Barrucand (Pierre). – Sur la distribution empirique des sommes de trois cubes ou de quatre bicarrés. *Comptes-Rendus de l'Académie des Sciences*, vol. 267, 1968, pp. 409–411.
- [2] Bohman (Jan) and Fröberg (Carl-Erik). – Numerical investigation of Waring's problem for cubes. *BIT*, vol. 21, n° 1, 1981, pp. 118–122.
- [3] Brüdern (J.). – On Waring's problem for cubes. *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 109, n° 2, 1991, pp. 229–256.
- [4] Davenport (H.). – On Waring's problem for fourth powers. *Annals of Mathematics*, vol. 40, 1939, pp. 731–747.
- [5] Deshouillers (J.-M.), Hennecart (F.), and Landreau (B.). – 7 373 170 279 850. *Prépublication de l'UMR 9936*, 1996.
- [6] Deshouillers (J.-M.), Hennecart (F.), and Landreau (B.). – Sums of powers: an arithmetic refinement to the probabilistic model of Erdős and Rényi. *Prépublication de l'UMR 9936*, 1996.
- [7] Dickson (L.). – All integers except 23 and 239 are sums of eight cubes. *Bulletin of the American Mathematical Society*, vol. 45, 1939, pp. 588–591.
- [8] Erdős (P.) and Rényi (A.). – Additive properties of random sequences of positive integers. *Acta Arithmetica*, vol. 6, 1960, pp. 83–110.
- [9] Halberstam (Heini) and Roth (Klaus Friedrich). – *Sequences*. – Springer-Verlag, New York-Berlin, 1983, 2nd edition.
- [10] Hardy (G. H.) and Ramanujan (S.). – Asymptotic formulæ in combinatory analysis. *Proceedings of the London Mathematical Society*, vol. 16, 1917, pp. 75–115.
- [11] Hilbert (D.). – Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n -ter Potenzen (Waring'sche Problem). *Mathematische Annalen*, vol. 67, 1909, pp. 281–300.
- [12] Hooley (Christopher). – On some topics connected with Waring's problem. *Journal für die Reine und Angewandte Mathematik*, vol. 369, 1986, pp. 110–153.
- [13] Landau (E.). – Über die Einteilung der ... Zahlen in 4 Klassen. *Arch. Math. Phys.*, vol. 13, n° 3, 1908, pp. 305–312.
- [14] Landreau (Bernard). – Étude probabiliste des sommes de s puissances s -ièmes. *Compositio Mathematica*, vol. 99, n° 1, 1995, pp. 1–31.
- [15] Linnik (U. V.). – On the representation of large numbers as sums of seven cubes. *Mat. Sbornik*, vol. 12, n° 54, 1943, pp. 218–224.

- [16] McCurley (Kevin S.). – An effective seven cube theorem. *Journal of Number Theory*, vol. 19, n° 2, 1984, pp. 176–183.
- [17] Romani (F.). – Computations concerning Waring’s problem. *Calcolo*, vol. 19, n° 4, 1982, pp. 415–431.
- [18] Vaughan (R. C.). – Sums of three cubes. *Bulletin of the London Mathematical Society*, vol. 17, 1985, pp. 17–20.
- [19] Vaughan (R. C.). – On Waring’s problem for cubes. *Journal für die Reine und Angewandte Mathematik*, vol. 365, 1986, pp. 122–170.
- [20] Vaughan (R. C.). – On Waring’s problem for cubes II. *Journal of the London Mathematical Society*, vol. 39, n° 2, 1989, pp. 205–218.
- [21] Watson (G. L.). – A proof of the seven cube theorem. *Journal of the London Mathematical Society*, vol. 26, n° 2, 1951, pp. 153–156.
- [22] Western (A. E.). – Computations concerning numbers representable by four or five cubes. *Journal of the London Mathematical Society*, vol. 1, n° 2, 1926, pp. 244–251.