Sums of Seven Cubes

Samir Siksek

University of Warwick

15 October 2015

Waring, Jacobi and Dase

Let $k \ge 2$. A k-th power means the k-th power of a non-negative integer.

Conjecture (Waring, 1770)

Every integer is the sum of four squares, nine cubes, 19 biquadrates, ...

"At the request of Jacobi, the famous computer Dase constructed a table showing the least number of positive cubes whose sum is any p < 12000". Dickson

Über die Zusammensetzung der Zahlen aus ganzen positiven Cuben: nebst einer Tabelle für die kleinste Cubenanzahl, aus welcher jede Zahl bis 12000 zusammengesetzt werden kann.

5.

(Von Herrn C. G. J. Jacobi, + weiland Professor zu Berlin.)

n den "Meditationes Algebraicae von Eduard Waring (S. 349 der Sten Ausgabe. Cambridge 1782.)" wird der Satz ausgesprochen. dafs zur Zusammensetzung der Zahlen aus (ganzen positiven) Cuben deren nie mehr als 9, zur Zusammensetzung der Zahlen aus (ganzen) Biquadraten deren nie mehr als 19 er/ordert werden.

Der Satz, dafs jede ganze Zahl die Summe von 9 oder weniger ganzen positiven Cuben ist, wird durch eine im 14ten Bande dieses Journals mitgetheilte Tabelle bestätigt, welche für jede Zahl bis 3000 die kleinste Anzahl von ganzen positiven Cuben angiebt, aus welchen sie durch Addition zusammengesetzt werden kann. Diese Tabelle ergab zugleich den merkwürdigen Umstand, dafs die Zahlen, zu deren Zusammensetzung 9 oder 8 Cuben erfordert werden, sehr bald aufhören, und dafs die Zahlen, zu deren Zusammensetzung 7 Cuben gebraucht werden, gegen das Ende der Tabelle so spärlich vorkommen, dafs es wahrscheinlich wurde, auch sie würden über eine gewisse Gränze nicht hinausreichen, oder dafs alle Zahlen, welche diese Grenze übersteigen, aus 6 oder weniger ganzen positiven Cuben zusammengesetzt werden können. Ja selbst diejenigen Zahlen, zu deren Zusammensetzung man 6 Cuben braucht, kommen bereits gegen das Ende dieser Tabelle weniger häufig vor. Sollten auch diese Zahlen einmal gänzlich aufhören, so würde der Satz gelten, dafs alle Zahlen, welche eine gewisse Gränze übersteigen, die Summen von 5 oder weniger ganzen positiven Cuben sind.

Die Anwesenheit des durch seine bewundernswürdige Fertigkeit und Sicherheit berühmten Rechners Dase veranlafste mich vor einigen Jahren, denselben aufzufordern, eine ähnliche Tabelle, wie die erwähnte, in größerem Umfange, für alle Zahlen bis 12000, zu berechnen; wobei sich denn mehrere Fehler der früheren Tabelle ergaben. So wurde gefunden, dafs nicht blofs die eine 6

Crelle's Journal f. d. M. Bd. XLII. Heft 1,

41

42 5. C. G. J. Jacobi, üb. die Zusammensetzung der Zahlen aus ganz. pos. Cuben.

Zahl 23, sondern auch noch eine zweite, 239, zu ihrer Zusammensetzung 9 Cuben erfordert. Es waren ferner unter den 15 Zahlen, die nach Herrn *Dases* Rechnung aus *acht* und keiner kleinern Anzahl Cuben zusammengesetzt werden können, nemlich:

15 22 50 114 167 175 186 212

231 238 303 364 420 428 454,

die beiden Zahlen 231 und 303 nicht als solche aufgeführt, und dagegen die Zahl 239 irrthümlich darunter angegeben worden.

Die Zahlen, zu deren Zusammensetzung sieben Cuben erfordert werden, sind die folgenden:

Die Anzahl dieser Zahlen bis 3000 beträgt 103, von welchen in der fraheren Tafel 29 fehlen, wahrend bei 4 Zahlen irrthamlich die Cubenanzahl 7 angegeben ist. Man sieht daher, dafs auch in Bezug auf das fräher berechnete Intervall von 1 bis 3000 die von Herrn *Dase* berechnete Tafel als ganz neu zu betrachten ist.

In der frühren Tafel waren unter den im Vorstehenden angegehnen Zahlen die drei Zahlen 2299, 2426, 2660 ausgelassen, und deshalb in einem Intervall von über S00 Zahlen keine mehr gefunden worden, deren Zusammensetzung 7 Cuben erforderte; man hielt es daher für wahrscheinlich, dafs 2183 die letzte von diesen Zahlen sei. Aber man sieht, dafs es nach derselben noch 21 Zahlen giebt, die aus nicht weniger als 7 Cuben zusammengesetzt werden können. Nach der Zahl 5518 findet sich erst nach einem Intervall von über 2000 Zahlen eine solche Zahl (S042) wieder, und nach dieser ist, in einem Intervall von fist 4000 Zahlen, keine weiter gefunden worden, so dafs es sehr wahrscheinlich ist, *dafs alle Zahlen, welche die Zahl 8042 am Größe übertreffen, die Summe von 6 oder weniger*

Jacobi's Conjecture on Sums of Cubes

Conjecture (Jacobi, 1851)

- (Waring) Every positive integer is the sum of nine cubes.
- Every positive integer other than 23 and 239 is the sum of eight cubes.
- **O** Every positive integer other than

15, 22, 23, 50, 114, 167, 175, 186, 212, 231, 238, 239, 303, 364, 420, 428, 454

is the sum of seven cubes.

Every positive integer other than

7, 14, 15,..., 5818, 8042 (138 exceptions)

is the sum of six cubes.

Sufficiently large integers are sums of five cubes.

Conjectures for sums of five/four cubes



Conjecture (Deshouillers, Hennecart and Landreau, 2000)

There are exactly 113 936 676 positive integers which are not the sum of four cubes, the largest of which is 7 373 170 279 850.

Theorems: Nine Cubes

Theorem (Wieferich (1908), Kempner (1912))

Every positive integer is the sum of nine cubes.

Theoretical part of proof: every positive $N > 2.25 \times 10^9$ is the sum of nine cubes.

Computational part of proof: apply greedy algorithm to show that every $N \le 2.25 \times 10^9$ is the sum of nine cubes.

Fact:

$$N = \lfloor \sqrt[3]{N} \rfloor^3 + O(N^{2/3}).$$

Greedy Algorithm: To show that all positive integers $\leq K$ are sums of n cubes, show that all integers $\leq C \cdot K^{2/3}$ are sums of n - 1 cubes.

Two iterations of greedy algorithm bring the bound into the range \leq 40000 of von Sterneck's table (1902).

Theorems: Eight Cubes

Theorem (Landau (1911), Baer (1913), Dickson (1939))

Every positive integer except 23 and 239 is the sum of eight cubes.

Theoretical part of proof: every positive $N > 2.26 \times 10^{15}$ is the sum of eight cubes.

Computational part of proof: apply greedy algorithm to show that every $N \le 2.26 \times 10^{15}$ is the sum of eight cubes.

Miss Evelyn Garbe: Extended von Sterneck's tables to 123,000.

Theorems: Seven Cubes

Theorem (Linnik (1943), Watson (1951))

Every sufficiently large integer is the sum of seven cubes.

Theorem (Ramaré (2007)) Every integer > exp(524) ($\approx 3.72 \times 10^{227}$) is the sum of seven cubes.

Theorem (Deshouillers, Henncart and Landreau, 2000) Every $454 < N \le \exp(78.7)$ ($\approx 1.51 \times 10^{34}$) is the sum of seven cubes.

Theorem (Boklan and Elkies (2009), Elkies (2010)) Every positive even integer > 454 is the sum of seven cubes.

Maillet's Identity (1895)

Sacrifice two cubes to get a square: $(r + x)^3 + (r - x)^3 = 2r^3 + 6rx^2$.

Sacrifice six cubes to get a sum of three squares:

$$(r+x)^{3} + (r-x)^{3} + (r+y)^{3} + (r-y)^{3} + (r+z)^{3} + (r-z)^{3} = 6r^{3} + 6r(x^{2} + y^{2} + z^{2})^{3}$$

More friendly variant:

$$(r+1+x)^{3} + (r-x)^{3} + (r+1+y)^{3} + (r-y)^{3} + (r+1+z)^{3} + (r-z)^{3} = (6r+3)(r^{2}+r+1+\underbrace{x^{2}+x+y^{2}+y+z^{2}+z}_{}).$$

Theorem (Gauss)

Let $k \ge 0$ be even. There exist x, y, z such that

 $x^{2} + x + y^{2} + y + z^{2} + z = k.$

$$(r+1+x)^3 + (r-x)^3 + (r+1+y)^3 + (r-y)^3 + (r+1+z)^3 + (r-z)^3 = (6r+3)(r^2+r+1+x^2+x+y^2+y+z^2+z).$$

Let N be an odd integer. To show that N is the sum of seven cubes, find t, r, x, y, z such that

$$N - 8t^{3} = (\underbrace{6r + 3}_{m})(r^{2} + r + 1 + \underbrace{x^{2} + x + y^{2} + y + z^{2} + z}_{m}).$$

Choose *m* such that

• $m \equiv 3 \pmod{6}$ is a positive integer (and let r = (m-3)/6);

- 2 m squarefree;
- every prime divisor of m/3 is $\equiv 5 \pmod{6}$.

Let t satisfy $N \equiv 8t^3 \pmod{m}$. Then

$$\frac{N-8t^3}{m}-r^2-r-1$$

is an even integer.

"Well-known lemma"

Lemma

Let $9K/10 \le N \le K$ be an odd integer. Let m satisfy

- (i) *m* is squarefree; 3 | *m*;
- (ii) every prime divisor of m/3 is $\equiv 5 \pmod{6}$;
- (iii) $2.63K^{1/3} \le m \le 2.92K^{1/3}$.

Let $0 \le t < m$ satisfy $t^3 \equiv N/8 \pmod{m}$. Suppose $0 \le t < m/10$. Then N is the sum of seven cubes.

Fundamental Problem with lemma: t can be any integer in [0, m).

Standard solution: Perturb the identity to improve the inequalities.

Bombieri's
$$(u^2v^2s + wx)^3 + (u^2v^2s - wx)^3$$

identity $+ (v^2w^2s + uy)^3 + (v^2w^2s - uy)^3$
 $+ (w^2u^2s + vz)^3 + (w^2u^2s - vz)^3$
 $= 2(u^6v^6 + v^6w^6 + w^6u^2) + 6su^2v^2w^2(x^2 + y^2 + z^2)$

Ramaré. To express N as the sum of seven cubes:

- Let u, v, $w \equiv 5 \pmod{6}$ be prime, gcd(uvw, N) = 1;
- Let ℓ satisfy $\ell^3 \equiv 4N/u^6 v^6 \pmod{w^2}$, $\ell^3 \equiv 4N/v^6 w^6 \pmod{u^2}$, $\ell^3 \equiv 4N/w^6 u^6 \pmod{v^2}$.
- Let $s \equiv 5 \pmod{6}$ be divisible only by primes $\equiv 5 \pmod{6}$ such that $s \equiv \ell^2 \pmod{u^2 v^2 w^2}$.
- Impose several inequalities ...

A "large sieve extension of the Brun-Titchmarsh inequality" shows that the existence of suitable u, v, w, s for $N > \exp(524)$.

Boklan and Elkies. Use variants where $x^2 + y^2 + z^2$ is replaced by a positive definite ternary form unique in its genus.

Back to fundamentally useless lemma!

Lemma

Let $9K/10 \le N \le K$ be an odd integer. Let m satisfy

(i) *m* is squarefree; 3 | *m*;

(ii) every prime divisor of m/3 is $\equiv 5 \pmod{6}$;

(iii) $2.63K^{1/3} \le m \le 2.92K^{1/3}$.

Let $0 \le t < m$ satisfy $t^3 \equiv N/8 \pmod{m}$. Suppose $0 \le t < m/10$. Then N is the sum of seven cubes.

Example/Heuristic.

- Let *K* = exp(524). Can find 9993 values of *m* satisfying (i)−(iii) with prime divisors ≤ 1097.
- Given *N*, probability that a given *m* fails to show that *N* is the sum of seven cubes is 9/10.
- The expected number of N for which all these m fail is

 $(K/20) \cdot (9/10)^{9993} \approx 1.03 \times 10^{-231}.$

Reformulation with many values of m

For $x \in \mathbb{R}$ and $m \in \mathbb{Z}_{\geq 1}$. Define **quotient** and **remainder** by

 $Q(x,m) = \lfloor x/m \rfloor, \qquad R(x,m) = x - Q(x,m) \cdot m \qquad (R(x,m) \in [0,m)).$

Let $\operatorname{Bad}(m) = \{x \in \mathbb{R} : R(x,m) \in [m/10,m)\}.$

Reformulation with many values of m

For $x \in \mathbb{R}$ and $m \in \mathbb{Z}_{\geq 1}$. Define **quotient** and **remainder** by

$$Q(x,m) = \lfloor x/m \rfloor, \qquad R(x,m) = x - Q(x,m) \cdot m \qquad (R(x,m) \in [0,m)).$$

Let $\operatorname{Bad}(m) = \{x \in \mathbb{R} : R(x,m) \in [m/10,m)\}.$

Lemma

Let $9K/10 \le N \le K$ be an odd integer. Let m satisfy (i)-(iii). Let $t^3 \equiv N/8 \pmod{m}$. If N is **not** the sum of seven cubes then $t \in Bad(m)$.

Reformulation with many values of m

For $x \in \mathbb{R}$ and $m \in \mathbb{Z}_{\geq 1}$. Define **quotient** and **remainder** by

$$Q(x,m) = \lfloor x/m \rfloor, \qquad R(x,m) = x - Q(x,m) \cdot m \qquad (R(x,m) \in [0,m)).$$

Let
$$\operatorname{Bad}(m) = \{x \in \mathbb{R} : R(x,m) \in [m/10,m)\}.$$

Lemma

Let $9K/10 \le N \le K$ be an odd integer. Let m satisfy (i)–(iii). Let $t^3 \equiv N/8 \pmod{m}$. If N is **not** the sum of seven cubes then $t \in Bad(m)$.

Lemma

Let $9K/10 \le N \le K$ be odd. Let W be a set of integers m satisfying (i)–(iii). Let

$$M = \operatorname{lcm}(W), \quad \operatorname{Bad}(W) = \cap_{m \in W} \operatorname{Bad}(m).$$

Let $T^3 \equiv N/8 \pmod{M}$. If N is **not** the sum of seven cubes then $T \in Bad(W)$.

Definitions. Let W be a set of m satisfying (i)–(iii).

$$Bad(m) = \{x \in \mathbb{R} : R(x,m) \in [m/10,m)\} = \bigcup_{k \in \mathbb{Z}} km + [m/10,m),$$

and

$$M = \operatorname{lcm}(W), \qquad \operatorname{Bad}(W) = \cap_{m \in W} \operatorname{Bad}(m).$$

Heuristic. Given $x \in [0, M)$, the 'probability' that $x \in Bad(m)$ is 9/10. The 'probability' that $x \in Bad(W)$ is $(9/10)^{\#W}$ (assuming independence). Expect

$$\ell([0,M) \cap \mathsf{Bad}(\mathcal{W})) pprox M \cdot (9/10)^{\#\mathcal{W}}$$

Example. Let $K = \exp(524) \approx 3.72 \times 10^{227}$. Can find 9993 values of *m* satisfying (i)–(iii) with prime divisors ≤ 1097 . Then

$$M \approx 9.44 \times 10^{235}$$
.

Expect: $\ell([0, M) \cap \mathsf{Bad}(\mathcal{W})) \approx 5.25 \times 10^{-222}.$

Computing Bad(W) (or $[0, M) \cap Bad(W)$)

Lemma

Let $[A, B) \subseteq [0, M)$. (i) If $A \notin Bad(W)$ then there is an explicit $A < A' \leq B$ such that $[A, B) \cap Bad(W) = [A', B) \cap Bad(W)$. (ii) If $A \in Bad(W)$ then there is an explicit $A < A'' \leq B$ such that $[A, B) \cap Bad(W) = [A, A'') \bigcup ([A'', B) \cap Bad(W))$.

Heuristic. Number of iterations needed to compute $[A, B) \cap Bad(W)$ is $\approx 7(B - A)/K^{1/3}$.

Example continued. Number of iterations needed to compute $[0, M) \cap \text{Bad}(W)$ is $\approx 10^{161}$.

The Tower. Let M_0 , M_1 ,..., M_r satisfy $M_i | M_{i+1}$ and $M_r = M$. Let $\mathcal{W}_i = \{ m \in \mathcal{W} : m | M_i \}, \qquad \mathcal{U}_i = \mathcal{W}_{i+1} \setminus \mathcal{W}_i, \qquad p_i = M_{i+1}/M_i.$ $\pi : [0, M_{i+1}) \rightarrow [0, M_i), \qquad x \mapsto R(x, M_i).$

Observe

$$\pi^{-1}(I) = \bigcup_{k=0}^{p_i-1} (kM_i + I), \qquad I \subset [0, M_i).$$

Then

$$[0, \mathit{M}_{i+1}) \cap \mathsf{Bad}(\mathcal{W}_{i+1}) \ = \ \pi^{-1}\left(\left[0, \mathit{M}_{i}
ight) \cap \mathsf{Bad}(\mathcal{W}_{i})
ight) \cap \ \mathsf{Bad}(\mathcal{U}_{i}).$$

Heuristic. Number of steps needed to compute Bad(W) is

$$\frac{7}{K^{1/3}}(M_0 + M_1 \cdot 0.9^{\#\mathcal{W}_0} + M_2 \cdot 0.9^{\#\mathcal{W}_1} + \dots + M_r \cdot 0.9^{\#\mathcal{W}_{r-1}}).$$

Choose M_0, \ldots, M_r such that $M_0/K^{1/3}$ is not too big, and the terms $M_i \cdot 0.9^{\#W_{i-1}}$ dying quickly.

Example. Let $K = \exp(524) \approx 3.72 \times 10^{227}$. Can find 9993 values of *m* satisfying (i)–(iii) with prime divisors ≤ 1097 . Then

 $M \approx 9.44 \times 10^{235}$.

Computation shows that $[0, M) \cap Bad(W)$ is the union of 729 intervals and

$$\ell([0, M) \cap \mathsf{Bad}(\mathcal{W})) =$$
1245835103891227282270190365612369211785920530251524580853973827407412033198232\frac{9}{10}
$$\approx 1.25 \times 10^{78}.$$

All intervals are concentrated in small neighbourhoods of $(a/q) \cdot M$ with $q \leq 42$.

Proof Conclusion

Let $K = \exp(524) \approx 3.72 \times 10^{227}$. Recall $M \approx 9.44 \times 10^{235}$. Suppose $9K/10 \le N \le K$ is odd and **not** the sum of seven cubes. Then

$$N \equiv 8T^3 \pmod{M}, \qquad T \in \mathsf{Bad}(\mathcal{W}).$$

So, there is a/q with $q \leq 42$ such that

$$T = (a/q) \cdot M + \alpha, \qquad \alpha \text{ is small.}$$

Let $k = q\alpha = qT - aM \in \mathbb{Z}$. Then $k \equiv qT \pmod{M}$ and

$$q^3N \equiv 8(qT)^3 \equiv 8k^3 \pmod{M}$$
.

But

$$|q^3N - 8k^3| < M$$

Hence

$$q^3N=8k^3.$$

Summary: If N is not the sum of seven cubes then N is a cube!!!

Theorem

Building on Maillet, Linnik, Watson, Cook, McCurley, Bombieri, Ramaré, Boklan, Elkies, . . .

Theorem

Every positive integer other than

15, 22, 23, 50, 114, 167, 175, 186, 212, 231, 238, 239, 303, 364, 420, 428, 454

is the sum of seven cubes.

Proof took about 18000 hours of computation distributed over 59 processors.

Two Big Questions

- Can we trust the computation?
- Why is Bad(W) concentrated around $(a/q) \cdot M$ with q small?

An interval in Bad(W)

Recall. W be a set of positive integers m satisfying

- (i) m is squarefree; $3 \mid m$;
- (ii) every prime divisor of m/3 is $\equiv 5 \pmod{6}$;
- (iii) $2.63K^{1/3} \le m \le 2.92K^{1/3}$.

 $M = \operatorname{lcm}(\mathcal{W}), \qquad \operatorname{Bad}(m) = \{x \in \mathbb{R} : R(x, m) \in [m/10, m)\},$

and

$$\mathsf{Bad}(\mathcal{W}) = \cap_{m \in \mathcal{W}} \mathsf{Bad}(m).$$

Observe $R(M - 1, m) = m - 1 \in [m/10, m)$.

Observe $M - 1 \in \mathsf{Bad}(\mathcal{W})$. In fact $[M - m + m/10, M) \subset \mathsf{Bad}(m)$.

$$\therefore \left[\max_{m\in\mathcal{W}}(M-m+m/10),\;M
ight]\subset \mathsf{Bad}(\mathcal{W})\,.$$

Constructing another interval in Bad(W)

Observe gcd(M/m, 42) = 1. Thus $M/m \neq 6, 7, 8, 9, 10 \pmod{42}$.

$$\therefore \quad R\left(\frac{M}{m}, 42\right) \notin (5, 11).$$

$$R\left(\frac{M}{42},m\right) = \frac{1}{42}R(M,42m) = \frac{m}{42}R\left(\frac{M}{m},42\right) \notin \left(\frac{5}{42}m,\frac{11}{42}m\right).$$

For small α ,

$$R\left(\frac{M}{42}-\alpha,m\right)\notin\left(\frac{5}{42}m-\alpha,\frac{11}{42}m-\alpha\right)$$
.

Let

•

$$\alpha \in \left(\frac{5}{42}m, \frac{17}{105}m\right)$$
 (17/105 = 11/42 - 1/10).

Then

. .

$$R\left(\frac{M}{42}-\alpha, \ m\right)\notin\left(0,\frac{m}{10}\right).$$
$$\left(\frac{M}{42}-\frac{17}{105}m, \ \frac{M}{42}-\frac{5}{42}m\right)\subset \mathsf{Bad}(m).$$

Constructing another interval in Bad(W)

$$\therefore \quad \left(\frac{M}{42} - \frac{17}{105}m, \ \frac{M}{42} - \frac{5}{42}m\right) \subset \mathsf{Bad}(m).$$
$$\bigcap_{m \in \mathcal{W}} \left(\frac{M}{42} - \frac{17}{105}m, \ \frac{M}{42} - \frac{5}{42}m\right) \subset \mathsf{Bad}(\mathcal{W}).$$

Recall

· · .

· · .

$$2.63K^{1/3} \le m \le 2.92K^{1/3}$$
.

$$\underbrace{\left(\frac{M}{42} - \frac{4471}{10500} \mathcal{K}^{1/3}, \ \frac{M}{42} - \frac{73}{210} \mathcal{K}^{1/3}\right)}_{\text{length} \approx 0.78 \mathcal{K}^{1/3}} \subset \text{Bad}(\mathcal{W}).$$

Computational Check! One of the 729 intervals that make up Bad(W) is [u, v) where the end points u, v are

 $\mu = 38951736404235848747133490324215209602466648736532939755374$ 00307522458157015057896866138248711539766725792372969437373 71206769063932017310777324617938079775100516093231041460322 $490961793995991410145937421686204642056677472293123392066\frac{3}{12}$ v = 3895173640423584874713349032421520960246664873653293975537400307522458157015057896866138248711539766725792372969437373 71206769063932017310777324617938079775101078697615391607190 077739469387928238665618669912989320140106379011502569660.

t turns out that
$$\left(\frac{M}{42} - \frac{4471}{10500} \kappa^{1/3}, \ \frac{M}{42} - \frac{73}{210} \kappa^{1/3}\right) \subset [u, v).$$
$$\frac{(4471/10500 - 73/210) \cdot \kappa^{1/3}}{v - u} \approx 0.9994$$

Conclusion

Thank You!