Every multiple of 4 except 212, 364, 420, and 428 is the sum of seven cubes

Kent D. Boklan and Noam D. Elkies

Abstract. It is conjectured that every integer $N > 454$ is the sum of seven nonnegative cubes. We prove the conjecture when N is a multiple of 4.

1 Introduction

Waring famously asserted in his Meditationes Algebraicæ of 1770:[1]

Omnis integer numerus vel est cubus, vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubis compositus . . .

meaning that every positive integer is the sum of at most nine positive cubes (equivalently, of exactly nine nonnegative cubes). A proof of this was given by Wieferich in 1909 (with an error later patched by Kempner [1912]). Landau then proved that only a finite set requires nine cubes, and Dickson [1939] identified this set with $\{23, 239\}$. Linnik then established, ineffectively, that only a finite set requires eight cubes, and seven suffice after some point [Linnik 1943]. In 1984, McCurley gave an effective proof of Linnik's result, demonstrating that every integer larger than $\exp(\exp(13.94))$ is the sum of seven positive cubes [McCurley 1984]. This was recently reduced to $\exp(524)$ [Ramaré 2007] using an analytic sieve argument.

It is believed that the exceptional set for Linnik's seven cubes theorem is

$$\{15, 22, 23, 50, 114, 167, 175, 186, 212, \qquad (1)$$
$$231, 238, 239, 303, 364, 420, 428, 454\}.$$

(Indeed one expects that every sufficiently large integer is the sum of four positive cubes [Deshouillers et al. 2000], but even such a statement with four replaced by six is well beyond our ability to prove.)

In the other direction, it is shown in [Bertault–Ramaré–Zimmermann 1999, Theorem 1 and Lemma 3] that if $454 < N < 2.5 \cdot 10^{26}$ then N is the sum of cubes of seven nonnegative integers; and it is observed in [Ramaré 2007, p.60] that

---

[1] Ellison [1971, p.10] reports that this statement appears on pages 203–204 of the 1770 edition. In the English translation [Waring 1782] of the 1782 edition, this statement appears on page 336 as part (9) of "Theorem 9"; see also the discussion on page 379 of the same translation, and the first section of [Ramaré 2007] for a fuller treatment of the history of this problem than we give here.

the computation reported in [Deshouillers et al. 2000, 433–434] raises the upper bound to $\exp(78.7) > 10^{34}$. But the computation to raise this bound to $\exp(524)$, and thus prove that (1) is the full exceptional set, remains utterly infeasible.

We give a different kind of partial result, where N is restricted by a congruence condition but not by size:

Theorem. *Every multiple of* 4 *except* 212, 364, 420, *and* 428 *can be written as the sum of seven nonnegative cubes.*

This is not the first such result, but the only earlier work in this direction that we know of is the proof in [Bertault–Ramaré–Zimmermann 1999] that if $N \equiv 0$ or $\pm 1 \bmod 9$ and N is an invertible cubic residue mod 37 then N is the sum of seven nonnegative cubes. Bertault et al. note that 37 could be replaced by various larger primes congruent to 1 mod 3. But the condition mod 9 is essential, and restricts N mod 9 to the three most common residues for a sum of seven cubes.[2] Compared with [Bertault–Ramaré–Zimmermann 1999], our new ingredient is the use of a quadratic form $Q = \sum_{i=1}^{3} c_i X_i^2$ with $(c_1, c_2, c_3) \neq (1, 1, 1)$ which is nevertheless known to represent all positive integers in certain arithmetic progressions.

The rest of the paper is organized as follows. We review the basic identity (4) for writing suitable integers as sums of six integer cubes, then give a criterion (Proposition 1) under which the cubes are positive. The criterion requires an auxiliary prime $p \equiv 2 \bmod 3$ in an interval $(AN^{1/3}, BN^{1/3})$ and a small enough positive integer x_0 such that $p|N - x_0^3$. We then choose c_1, c_2, c_3 and show that a suitable x_0 exists provided p satisfies a congruence condition mod 72. Finally we use the explicit bounds of [Ramaré–Rumely 1996] on the distribution of primes in arithmetic progressions, plus a short further computation of prime chains, to prove that such p exists if $N > N_0 = 10^{18}$. This completes the proof because that N_0 is well below the threshold of $2.5 \cdot 10^{26}$ of [Bertault–Ramaré–Zimmermann 1999].

Since we formulate the proof so as to use only positive rather than nonnegative cubes, we automatically get a representation of N as a sum of seven positive cubes for all $N > 10^{18}$ divisible by 4. For $N \leq 10^{18}$, there are cases not listed in (1) for which N is a sum of six or fewer nonnegative cubes but not exactly seven; the largest of these is apparently 2408 (as it happens a multiple of 4),

---

[2] The following table gives the distribution mod 9 of $N = n_1^3 + n_2^3 + \ldots + n_7^3$ among the 9^7 possibilities of $(n_1, n_2, \ldots, n_7) \bmod 9$:

$N \bmod 9$	0	± 1	± 2	± 3	± 4
proportion	17.97%	16.32%	12.21%	7.68%	4.80%

Note that of the seventeen exceptions listed in (1), eleven are congruent to ± 4 mod 9, and the remaining six to -3 mod 9. These rare residues ± 3, ± 4 are also the least easily accessible to current approaches to the seven-cube problem, including ours: it will be seen that we must work hardest to prove our theorem for N congruent to ± 3 or ± 4 mod 9. Note that while our condition $4|N$ also puts N in a probabilistically favored congruence class, the discrepancy is minuscule: a random sum of seven cubes is divisible by 4 with probability only 25.39%.

whose only representations as a sum of seven or fewer positive cubes are

$$
\begin{aligned}
2408 &= 10^3 + 10^3 + 7^3 + 4^3 + 1^3 \\
&= 12^3 + 8^3 + 5^3 + 3^3 + 2^3 + 2^3 \\
&= 11^3 + 8^3 + 6^3 + 6^3 + 5^3 + 2^3 \\
&= 10^3 + 10^3 + 6^3 + 4^3 + 4^3 + 4^3 \qquad (2)
\end{aligned}
$$

and permutations of these four sums.

2 A six cube identity

The use of the identities equivalent to the following Lemma and its Corollary to study sums of seven cubes goes back at least as far as [Linnik 1943, §2].

Lemma 1. *Let*

$$
Q = \sum_{i=1}^{3} c_i X_i^2, \qquad C = \sum_{i=1}^{3} c_i^3. \qquad (3)
$$

Then

$$
\sum_{i=1}^{3} \left((c_i p + X_i)^3 + (c_i p - X_i)^3 \right) = 2Cp^3 + 6pQ. \qquad (4)
$$

Proof: Apply the identity $(r+s)^3 + (r-s)^3 = 2r^3 + 6rs^2$ to each of the three terms in the sum. $\qquad \square$

Corollary. *If p and the c_i are positive integers and the X_i are integers such that $|X_i| < c_i p$ for each i, then $2Cp^3 + 6pQ$ is the sum of cubes of six positive integers.* $\qquad \square$

3 Strategy

Given N, we choose integers $c_i > 0$ and a prime $p \equiv 2 \bmod 3$ of size roughly $N^{1/3}$, and let x_0 be a small nonnegative integer such that $N - x_0^3 = 2Cp^3 + 6pQ_0$ for some integer $Q_0 \geq 0$. Such an x_0 exists if N/p^3 is large enough because every integer is a cube mod $6p$. If, moreover, x_0 can be chosen such that Q_0 is represented by the quadratic form Q, and N/p^3 is small enough so that all the terms in the sum in the identity (4) are positive, then we can use that identity to write N as the sum of cubes of seven positive integers.

Because no ternary quadratic form represents all $Q_0 \geq 0$, we may need to put a further congruence condition on x_0 modulo some β relatively prime to $6p$; we shall then choose the least $x_0 > 0$ satisfying these congruences, so that $x_0 \leq 6\beta p$. We find that this imposes the following lower and upper bounds on N/p^3:

Proposition 1 *Let c_1, c_2, c_3 be positive integers with $c_1 = \min c_i$. Set $C =$*

$\sum_{i=1}^{3} c_i^3$. *For some $\beta \geq 1$ assume that*

$$2C + 216\beta^3 < \frac{N}{p^3} < 2C + 6c_1^3. \tag{5}$$

If x_0 is a positive integer such that $x_0 \leq 6\beta p$ and

$$N - x_0^3 = 2Cp^3 + 6pQ_0, \tag{6}$$

then $Q_0 > 0$; if further

$$Q_0 = c_1 X_1^2 + c_2 X_2^2 + c_3 X_3^2 \tag{7}$$

for some integers X_i, then N is the sum of cubes of seven positive integers.

Proof: The lower bound on N/p^3 assures that

$$N - x_0^3 \geq N - (6\beta p)^3 > 2Cp^3,$$

so $Q_0 > 0$. Given a solution of (7), we use the identity (4) to write $N - x_0^3$ as the sum of cubes of six integers. Since $x_0 \geq 0$, it thus suffices to verify that $|X_i| < c_i p$. Indeed we have

$$c_i X_i^2 \leq Q_0 = \frac{N - x_0^3 - 2Cp^3}{6p} \leq \frac{N - 2Cp^3}{6p} < \frac{6c_1^3 p^3}{6p} = c_1^3 p^2 \leq c_i^3 p^2$$

so $X_i^2 < c_i^2 p^2 = (c_i p_i)^2$. Since $c_i p > 0$, we are done. $\qquad\square$

The inequalities (5) require

$$\beta < c_1/\sqrt[3]{36}. \tag{8}$$

Assuming this condition holds, (5) restricts p to an interval $(AN^{1/3}, BN^{1/3})$ for some constants A, B with $0 < A < B$. We then use explicit bounds for the distribution of primes in arithmetic progressions to find $N_0 < 10^{26}$ such that a suitable p exists for all $N \geq N_0$.

When N is a multiple of 4 but not of 8, we shall need to impose a condition on $p \bmod 8$; when N falls in one of the hardest residue classes $\pm 4 \bmod 9$, we shall also impose a condition on $p \bmod 9$.

4 Choices and analysis

We choose $(c_1, c_2, c_3) = (4\beta, 4\beta, 6\beta)$ where $\beta = 1$ or $\beta = 5$ depending on the residue of $N \bmod 9$ (as specified later in this section). Then condition (8) is satisfied, and

$$c_1 X_1^2 + c_2 X_2^2 + c_3 X_3^2 = 2\beta(2X_1^2 + 2X_2^2 + 3X_3^2). \tag{9}$$

We calculate $C = 344\beta^3$, whence $A = \beta^{-1}/\sqrt[3]{1072}$ and $B = \beta^{-1}/\sqrt[3]{904}$, with ratio $B/A = (134/113)^{1/3} > 1.0584$.

We choose x_0 so that

$$x_0^3 \equiv N - 2Cp^3 = N - 688(\beta p)^3 \bmod 6\beta p, \tag{10}$$

which is possible because every integer is a cube mod $6\beta p$. We select the least positive x_0 satisfying this congruence; thus $x_0 \leq 6\beta p$. As N and $6\beta p$ are even, so is x_0. Since also $4|N$ and $2|C$, while β and p are odd, it follows that $N - 2Cp^3$ is a multiple of $12\beta p$. That is,

$$Q_1 := \frac{N - x_0^3 - 688(\beta p)^3}{12\beta p} \tag{11}$$

is an integer.

This integer Q_1 is positive by our Proposition. Set $Q_0 = 2\beta Q_1$. In view of (9), we need Q_1 to be represented by the quadratic form $2X_1^2 + 2X_2^2 + 3X_3^2$. This quadratic form is unique in its genus, so it represents all nonnegative integers that are not excluded by congruence conditions. In this case this means all Q_1 that are neither congruent to 1 mod 8 nor of the form $9^t(9m + 6)$ for some nonnegative integers m, t. (See [Dickson 1927, (16), pages 44–45] for this characterization of the integers represented by Q_1.) It remains to choose p so that these conditions are satisfied.

The condition for Q_1 mod 8 holds automatically if $N \equiv 0$ mod 8, because then the numerator $N - x_0^3 - 688(\beta p)^3$ in (11) is a multiple of 8 while the denominator is not, so the quotient Q_1 is even. Assume then that $N \equiv 4$ mod 8. Since $688 \equiv 16$ mod 32 and βp is odd, we have $688(\beta p)^3 \equiv 16$ mod 32 as well. Since x_0 is even, x_0^3 is a multiple of 8 *not* congruent to 16 mod 32. Therefore

$$\frac{N - x_0^3 - 688(\beta p)^3}{4} \not\equiv \frac{N}{4} \bmod 8. \tag{12}$$

We therefore choose p so that

$$3\beta p \equiv \frac{N}{4} \bmod 8, \tag{13}$$

and this guarantees that $Q_1 \not\equiv 1$ mod 8, so Q_1 passes the mod-8 test for representability by the quadratic form $2X_1^2 + 2X_2^2 + 3X_3^2$.

Next we ensure that $Q_1 \neq (9m + 6)9^t$ by choosing $\beta \in \{1, 5\}$ and p mod 9 so that $Q_1 \not\equiv 0, 6$ mod 9. Since $p \equiv 2$ mod 3 implies $p^3 \equiv -1$ mod 9, the choice of β determines $688(\beta p)^3$ mod 9. Thus, as $688 \equiv 4$ mod 9, we have

$$N - 688(\beta p)^3 \equiv N + 4\beta^3 \bmod 9. \tag{14}$$

Now $x_0^3 \equiv 0$ or ± 1 mod 9 for all integers x_0. Therefore if

$$N + 4\beta^3 \not\equiv 0 \text{ or } \pm 1 \bmod 9 \tag{15}$$

then $N - x_0^3 - 688(\beta p)^3$ cannot be a multiple of 9, whence Q_1 is not a multiple of 3, so *a fortiori* not congruent to 0 or 6 mod 9. We have $\beta^3 \equiv 1$ mod 9 for

$\beta = 1$, and $\beta^3 \equiv -1 \bmod 9$ for $\beta = 5$; thus, unless $N \equiv \pm 4 \bmod 9$, we may choose β so that N satisfies condition (15)

In the remaining cases $N \equiv \pm 4 \bmod 9$, we choose β so that $3|x_0$ by requiring $\beta = 5$ for $N \equiv 4 \bmod 9$ and $\beta = 1$ for $N \equiv -4 \bmod 9$. Then $27|x_0^3$, and the numerator $N - x_0^3 - 688(\beta p)^3$ in (11) is a multiple of 9 that we can control mod 27 by choosing p mod 9. Indeed if $\beta p = 3k \pm 1$ then $(\beta p)^3 \equiv 9k \pm 1 \bmod 27$. Since $688 \equiv 13 \bmod 27$ this gives

$$\frac{N - x_0^3 - 688(\beta p)^3}{9} \equiv \frac{N \pm 13}{9} - k \bmod 3, \tag{16}$$

with the sign chosen so that $9|N \pm 13$. Dividing by $4\beta p$, we conclude that

$$\frac{Q_1}{3} \equiv \beta\left(k - \frac{N \pm 13}{9}\right) \bmod 3. \tag{17}$$

We thus choose $k \equiv \beta + ((N \pm 13)/9) \bmod 3$. That is,

$$\beta p \equiv 3\beta + \frac{N \pm 13}{3} \pm 1 \bmod 9, \tag{18}$$

with the sign in ± 1 chosen so that $\pm 1 \equiv -\beta \bmod 3$. Then $Q_1/3 \equiv 1 \bmod 3$, so Q_1 passes the mod-9 test for representability by $2X_1^2 + 2X_2^2 + 3X_3^2$.

5 Conclusion

To finish the proof of our Theorem, we show:

Lemma 2. *For $\beta \in \{1, 5\}$ let $A = \beta^{-1}/\sqrt[3]{1072}$ and $B = \beta^{-1}/\sqrt[3]{904}$. Set $N_0 = 10^{18}$. Then whenever $N > N_0$ there exists a prime $p \in (AN^{1/3}, BN^{1/3})$ in each odd congruence class $l \bmod 72 = 8 \cdot 9$ with $l \equiv 2 \bmod 3$.*

This will suffice because 10^{18} is smaller than the lower bound of $2.5 \cdot 10^{26}$ of [Bertault–Ramaré–Zimmermann 1999] on an integer N not listed in (1) that is not the sum of seven nonnegative cubes.

Proof: Taking $k = 72$ in [Ramaré–Rumely 1996, Theorem 1], we find that for every prime $p > 10^{10}$ there exists a prime $p' > p$ such that $p' \equiv p \bmod 72$ and $p' \leq ((1 + \epsilon_{72})/(1 - \epsilon_{72}))p$. Consulting [Ramaré–Rumely 1996, §5, p.419, Table 1], we find $\epsilon_{72} < 0.013$, so $(1 + \epsilon_{72})/(1 - \epsilon_{72}) < 1.027$ which is well below the gap ratio of $B/A = (134/113)^{1/3} > 1.0584$ that we need. This establishes Lemma 2 for $N > 1072(5 \cdot 10^{10})^3$.

That bound is not small enough for our application because it exceeds the threshold of [Bertault–Ramaré–Zimmermann 1999] and even (by a factor of 13.4) the improved bound of 10^{34} reported in [Ramaré 2007, p.60]. But it reduces the proof of Lemma 2 to a finite computation. To make this computation manageable, we prove:

Sublemma. *In each congruence class $l \bmod 72$ coprime to 72 there exist an integer M_l and primes p_i $(0 \leq i \leq M_l)$ such that $p_0 < 19541$, $p_{i-1} < p_i < 1.0584 p_{i-1}$ for each $i = 1, 2, \ldots, M_l$, and $p_{M_l} > 10^{10}$.*

6

To derive Lemma 2 from this Sublemma, let p be the smallest prime such that $p \equiv l \bmod 72$ and $p > AN^{1/3}$. Then $p > 19541$ because

$$N > N_0 = 10^{18} > 1072(5 \cdot 19541)^3.$$

If $p > 10^{10}$, use [Ramaré–Rumely 1996]. Else apply the Sublemma and find the maximal nonnegative $i < M_l$ such that $p > p_i$. Then

$$p \leq p_{i+1} < 1.0584\, p_i < 1.0584\, p < 1.0584\, AN^{1/3} < BN^{1/3},$$

and we are done.

(Conversely, the existence of the gap ratio $17573/16493 < 1.0655$ between the primes 16493 and 17573 congruent to 5 mod 72 shows that N_0 cannot be brought much below 10^{18} in Lemma 1.)

To find the primes p_i required by the Sublemma, we run the following algorithm for each l with some choice of positive $\delta < 0.0584$:

- Let p_0 be the largest prime $p < 19541$ such that $p \equiv l \bmod 72$. Set $i = 0$.

- While $p_i < 10^{10}$, let p_{i+1} be the least prime such that $p_{i+1} \equiv p_i \bmod 72$ and $p_{i+1} > (1+\delta)p_i$, and increment i to $i+1$.

Each "largest prime" and "least prime" is found by simply stepping down or up the congruence class until a prime is found. The second step is repeated at most $\log(10^{10})/\log(1+\delta) \doteq 23/\delta$ times. Once p_i exceeds 10^{10}, we succeed if $\max_{i < M_l} p_{i+1}/p_i < 1.0584$; otherwise we try again for a smaller δ: decreasing δ lengthens the computation but skips fewer primes. We find that $\delta = 0.01$ is small enough for the computation to succeed for each l. Then $M_l < 1250$ in each case, and the largest p_{i+1}/p_i ratio occurs at $(l,i) = (5,1)$, namely $21101/19949 < 1.0578 < 1.0584$. This computation, programmed in PARI-GP [Batut et al. 1998], takes less than a minute to run on an office desktop machine (G5 PowerMac with a 1.8 GHz processor), and completes the proof of the Sublemma and thus of our Theorem.

Remark: We could also have used [Ramaré–Rumely 1996, Corollary 5.2.2] to prove a result similar to Lemma 2 but with the weaker bound $N_0 = 10^{21}$, which is still good enough because $10^{21} < 2.5 \cdot 10^{26}$. But this would implicitly rely on the much more extensive calculations by Ramaré and Rumely of the distribution in arithmetic progressions of the primes up to 10^{10}, which involve the computation of hundreds of millions of primes, whereas we needed fewer than $1250\,\phi(72) = 3 \cdot 10^4$ primes to prove Sublemma 2.

References

[Batut et al. 1998] Batut, C., Belabas, K. Bernardi, D., Cohen, H., and Olivier, M.: *User's Guide to PARI-GP*, available from `http://megrez.math.u-bordeaux.fr/pub/pari` .

[Bertault–Ramaré–Zimmermann 1999] Bertault, F., Ramaré, O., and Zimmermann, P.: On sums of seven cubes. *Math. Comp.* **68** (1999) #227, 1303–1310.

[Deshouillers et al. 2000] Deshouillers, J.-M., Hennecart, F., and Landreau, B.: 7 373 170 279 850 (with an appendix by I. Gusti Putu Purnaba), *Math. Comp.* **69** #229 (2000), 421–439.

[Dickson 1927] Dickson, L. E.: Quaternary Quadratic Forms Representing all Integers. *Amer. J. Math.* **49** #1 (1927), 39–56.

[Dickson 1939] Dickson, L.E.: All integers except 23 and 239 are the sums of 8 cubes. *Bull. Amer. Math. Soc.* **45** (1939), 588–591.

[Ellison 1971] Ellison, W.J.: Waring's problem. *Amer. Math. Monthly* **78** (1971), 10–36.

[Kempner 1912] Kempner, A.J.: Uber das Waringsche Problem und einige Verallgemeinerunden. *Diss. Göttingen* (1912) Extract in *Math. Annalen* **72** (1912), 387.

[Linnik 1943] Linnik, U. V.: On the representation of large numbers as sums of seven cubes. *Rec. Math. [=Mat. Sbornik] N.S.* **12(54)** (1943), 218–224.

[McCurley 1984] McCurley, K. S.: An effective seven cubes theorem. *J. Number Theory* **19** (1984) #2, 176–183.

[Ramaré 2007] Ramaré, O.: An explicit result of the sum of seven cubes. *Manuscripta Math.* **124** (2007), 59–75.

[Ramaré–Rumely 1996] Ramaré, O., and Rumely, R.: Primes in arithmetic progressions. *Math. Comp.* **65** (1996) #213, 397–425.

[Waring 1782] Waring, E.: *Meditationes Algebraicæ* [3rd ed. (1782)]: an English translation of the work of Edward Waring, edited and translated from the Latin by Dennis Weeks. Providence, RI: Amer. Math. Soc., 1991.

KDB: Department of Computer Science, Queens College, Flushing, NY 11367, U.S.A. (boklan@boole.cs.qc.edu)

NDE: Department of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A. (elkies@math.harvard.edu)