On Sums of Four Cubes

Henri Cohen

March 18, 2004

Abstract

We give a translation of a paper of Demjanenko proving that every integer not congruent to ± 4 modulo 9 is a sum of four positive or negative cubes.

1 The main result

In this paper, an integer will always be an element of $\mathbb{Z}$, and when we speak of sums of cubes, we always mean cubes of elements of $\mathbb{Z}$, in other words positive or negative cubes. The main result of this paper, due to Demjanenko, is the following:

Theorem 1.1 *Every integer n such that $n \not\equiv \pm 4 \pmod 9$ is a sum of four cubes.*

Note that it is conjectured that the restriction $n \not\equiv \pm 4 \pmod 9$ is unnecessary, but this seems out of reach with present methods.

The plan of the proof is as follows. First, if n belongs to a number of residue classes, polynomial identities immediately imply that n is a sum of four cubes of integers, each integer being in fact a polynomial of degree 1 or 2 in n. Thanks to these identities, we are reduced to $n \equiv \pm 38 \pmod{108}$. We then introduce the prime number $p = 3323$ and we show by another explicit identity involving polynomials of degree 2 in n that if $p \mid n$, then n is a sum of four cubes. To treat the remaining cases where $p \nmid n$, we use the explicit solution to a Pell equation and show that every nonzero congruence class modulo p is attained as a sum of four cubes. The integers which occur here are not anymore polynomials in n.

2 The "easy" congruence classes

Proposition 2.1 *Every integer n such that $n \not\equiv \pm 4 \pmod 9$ and $n \not\equiv \pm 38 \pmod{108}$ is a sum of four cubes.*

Proof. The identities

$$6x = (x-1)^3 + (-x)^3 + (-x)^3 + (x+1)^3 \text{ and}$$
$$6x + 3 = x^3 + (-x+4)^3 + (2x-5)^3 + (-2x+4)^3 = 6x + 3$$

show that every multiple of 3 is a sum of four cubes. Next the identities

$$\begin{aligned}
18x+1 &= (2x+14)^3 + (-2x-23)^3 + (-3x-26)^3 + (3x+30)^3 \ , \\
18x+7 &= (x+2)^3 + (6x-1)^3 + (8x-2)^3 + (-9x+2)^3 \ , \\
18x+8 &= (x-5)^3 + (-x+14)^3 + (-3x+29)^3 + (3x-30)^3 \ ,
\end{aligned}$$

together with the complementary identities obtained by changing x into $-x$ and multiplying by -1 show that every $n \equiv \pm 1$, ± 7 or ± 8 modulo 18 is a sum of four cubes. Since we exclude $n \equiv \pm 4 \pmod 9$ the only remaining congruence classes to examine are $n \equiv \pm 2 \pmod{18}$.

The identities

$$\begin{aligned}
54x+2 &= (29484x^2 + 2211x + 43)^3 + (-29484x^2 - 2157x - 41)^3 \\
&\quad + (9828x^2 + 485x + 4)^3 + (-9828x^2 - 971x - 22)^3 \\
54x+20 &= (3x-11)^3 + (-3x+10)^3 + (x+2)^3 + (-x+7)^3 \\
216x-16 &= (14742x^2 - 2157x + 82)^3 + (-14742x^2 + 2211x - 86)^3 \\
&\quad + (4914x^2 - 971x + 44)^3 + (-4914x^2 + 485x - 8)^3 \\
216x+92 &= (3x-164)^3 + (-3x+160)^3 + (x-35)^3 + (-x+71)^3
\end{aligned}$$

together with their complementary identities leave the congruence classes $n \equiv \pm 38 \pmod{108}$, proving the proposition. □

To prove that every integer not congruent to ± 4 modulo 9 is a sum of four cubes it is thus sufficient to consider $n \equiv \pm 38 \pmod{108}$, and if necessary changing n into $-n$ and the cubes into their opposite, we may assume that $n \equiv 38 \pmod{108}$. We distinguish between the cases $3323 \mid n$ and otherwise.

3 Proof of Demjanenko's theorem

3.1 The Case $3323 \mid n$

Note that 3323 is a prime number.

Proposition 3.1 *If* $n \equiv \pm 38 \pmod{108}$ *and* $3323 \mid n$ *then* n *is a sum of four cubes.*

Proof. Clearly $n \equiv 38 \pmod{108}$ is equivalent to $n/3323 \equiv 38 \cdot 3323^{-1} \equiv 46 \pmod{108}$, so the proposition is an immediate consequence of the identity

$$\begin{aligned}
3323(108x+46) &= (29484x^2 + 25143x + 5731)^3 + (-29484x^2 - 25089x - 5708)^3 \\
&\quad + (9828x^2 + 8129x + 1802)^3 + (-9828x^2 - 8615x - 2009)^3 \ .
\end{aligned}$$

□

3.2 The Case $3323 \nmid n$

Proposition 3.2 *If* $n \equiv \pm 38 \pmod{108}$ *and* $3323 \nmid n$ *then* n *is a sum of four cubes.*

Proof. Let a, b, k be integers and set

$$x = 24k + 163a + 7563b,\ y = -(27k + 173a + 7309b),$$
$$z = 19k + 89a + 2693b,\ t = -(10k - a + 2b)\ .$$

We check that $x^3 + y^3 + z^3 + t^3 = -59814(a^2 - 3420b^2)k + P(a, b)$, with

$$P(a, b) = (a - 2b)^3 + (163a + 7563b)^3 + (-173a - 7309b)^3 + (89a + 2693b)^3\ .$$

Thus, if a and b are chosen as solutions of the Pell equation $a^2 - 3420b^2 = 1$ we have $x^3 + y^3 + z^3 + t^3 = -59814k + P(a, b)$. Since $59814 = 2 \cdot 3^2 \cdot 3323$, given such a pair (a, b) the equation $x^3 + y^3 + z^3 + t^3 = n$ is solvable in k if and only if $P(a, b) \equiv n$ modulo 2, 9 and 3323. Since $n \equiv 2 \pmod{18}$, the condition modulo 2 is $2 \mid b$, and the condition modulo 9 is easily seen to be $a \equiv 1 \pmod 3$ and $3 \mid b$. Thus the condition modulo 18 is $a \equiv 1 \pmod 6$ and $b \equiv 0 \pmod 6$. There remains the condition modulo 3323.

The fundamental unit of the order $\mathbb{Z}[\sqrt{3420}]$ is easily computed to be $\varepsilon = 3041 + 52\sqrt{3420}$, which is of norm 1. Thus $a + b\sqrt{3420} = s\varepsilon^k$ for any $k \in \mathbb{Z}$ and some $s = \pm 1$, in other words

$$a = s\frac{\varepsilon^k + \overline{\varepsilon}^k}{2} \quad \text{and} \quad b = s\frac{\varepsilon^k - \overline{\varepsilon}^k}{2\sqrt{3420}}\ .$$

Since a and b satisfy a second order linear recurrence, it is immediately seen that the condition $6 \mid b$ is equivalent to $3 \mid k$, and then we have $a \equiv \pm 1 \pmod 6$, so $a \equiv 1 \pmod 6$ can be achieved by choosing $s = (-1)^k$, so that setting $\eta = -\varepsilon^3$ we have for some integer m

$$a = \frac{\eta^m + \overline{\eta}^m}{2} \quad \text{and} \quad b = \frac{\eta^m - \overline{\eta}^m}{2\sqrt{3420}}\ .$$

Now we note that $3420 \equiv 97^2 \pmod{3323}$, hence $\varepsilon \equiv 2046 \pmod{3323}$ hence $\eta \equiv 3231 \pmod{3323}$ and $\overline{\eta} \equiv 2420 \pmod{3323}$, so that

$$a \equiv \frac{3231^m + 2420^m}{2} \pmod{3323} \text{ and } b \equiv \frac{3231^m - 2420^m}{2 \cdot 556} \pmod{3323}\ .$$

Replacing gives

$$P(a, b) \equiv 889 \cdot 3231^m \pmod{3323}\ .$$

Now it is immediately checked that 3231 is a primitive root modulo 3323. Since $\gcd(889, 3323) = 1$ it follows that for any n such that $3323 \nmid n$ there exists $m \in \mathbb{Z}$ with $889 \cdot 3231^m \equiv n \pmod{3323}$, hence there exists a and b such that $P(a, b) \equiv n \pmod{3323}$, proving that the condition modulo 3323 can be satisfied and finishing the proof of the proposition, hence of the theorem. □

Remark. I have no idea how one obtains the second degree identities used in the beginning of the proof (although they are clearly related to one another and to the identity for $18x + 8$), and why we set x, y, z and t as given (why use the identity $24^3 + (-27)^3 + 19^3 + (-10)^3 = 0$ among so many similar identities?). In other words, the proof that I have given above, which is a simple translation of Demjanenko's into English, is correct (I have checked all the identities on a computer), but I do not claim to understand it.

References

[1] V. Demjanenko, *On sums of four cubes*, Izvestia Vischik Outchetsnik Zavedenii Mathematika **54** (1966), 64–69.

Laboratoire A2X, U.M.R. 5465 du C.N.R.S.,
Université Bordeaux I, 351 Cours de la Libération,
33405 TALENCE Cedex, FRANCE
e-mail: cohen@math.u-bordeaux1.fr