Characterizing the Sum of Two Cubes Version: 18th December 2003.

Kevin A. Broughan

University of Waikato, Hamilton 2001, New Zealand,
kab@waikato.ac.nz

Abstract. An intrinsic characterization of positive integers which can be represented as the sum or difference of two cubes is given. Every integer has a smallest multiple which is a sum of two cubes and such that the multiple, in the form of an iterated composite function of the integer, is eventually periodic with period one or two. The representation of any integer as the sum of two cubes to a fixed modulus is always possible if and only if the modulus is not divisible by 7 or 9.

Sequence number a045980.
MSC 2000 11A07, 11B13, 11B50, 11D25, 11D79, 11P05.
Key words and phrases: sum of two cubes, diophantine equation.

1 Introduction

Consider the beautiful characterization of numbers which are the sum of two squares, namely [2, Theorem 366] a number n is the sum of two squares if and only if all the prime factors of n of the form $4m + 3$ have even exponent in the standard factorization of n. This is not matched by any known comparable condition for the sum of two cubes. In the absence of such a characterization there has been a great deal of interest in questions related to the sum of two cubes, see for example [6], [8].

In Section 2 we give an intrinsic characterization, a property of n itself, which will determine whether it is representable as the sum of two cubes or not. The characterization is not so simple but is complete, and covers both $n = x^3 + y^3$ and $n = x^3 - y^3$. To have a representation in either of these forms n must have a divisor m which satisfies strict conditions: $m^3 - n/m$ must be divisible by 3 with quotient l satisfying $m^2 + 4l$ is a perfect square. The applicable range for values of m and sign of l discriminates between the two equations $n = x^3 + y^3$ and $n = x^3 - y^3$.

In Section 3 the equation $n = x^3 + y^3$ modulo m is considered and the main result of the paper proved. The divisibility of m by 7 or 9 is definitive, in that it is in these cases, and **only** in these cases, that the form $n \equiv x^3 + y^3 \mod m$ does **not** have a solution for every n.

Every positive integer has a multiple which is the sum of two cubes. This phenonena is studied in Section 4 where functions, $\theta(n)$ and $\eta(n)$ giving the "minimum multiple" of an integer which represents the sum of two cubes, are defined.

These functions, when iterated, are eventually periodic with period length one or two.

2 Characterizing the sum of two cubes

Theorem 1. *Let n be a positive integer. Then the equation $n = x^3 + y^3$ has a solution in positive integers x and y if and only if the following three conditions are satisfied:*

1a. There exists a divisor $m \mid n$ with $n^{\frac{1}{3}} \leq m \leq 2^{\frac{2}{3}} n^{\frac{1}{3}}$ such that
2a. for some positive integer l, $m^2 - n/m = 3l$ and such that
3a. the integer $m^2 - 4l$ is a perfect square.

The conditions equivalent to the existence of a solution to $n = x^3 - y^3$ in positive integers are as follows:

1b. There exists a divisor $m \mid n$ with $1 \leq m < n^{\frac{1}{3}}$ such that
2b. for some positive integer l, $n/m - m^2 = 3l$ and such that
3b. the integer $m^2 + 4l$ is a perfect square.

Proof. First we show that if the equation $n = x^3 + y^3$ has a solution then (1a-3a) must be satisfied.

(1a) Let $n = u^3 + v^3 = (u + v)(u^2 - uv + v^2)$ in positive integers u, v and let $m = u + v$ so $m \mid n$. The form

$$x^2 - xy + y^2 = \frac{n}{m}$$

is the equation of an ellipse, called here E, with major axis the line $y = x$, and (u, v) is a point on the ellipse in the first quadrant.

The straight line $m = x + y$ cuts the x-axis at $x = m$ which is equal or to the right of the point where the ellipse cuts the axis, namely $x = \sqrt{n/m}$. Hence

$$\sqrt{\frac{n}{m}} \leq m \quad \Rightarrow \quad n^{\frac{1}{3}} \leq m \quad (1).$$

The length of the major axis of E is $\sqrt{2n/m}$ and the distance of the line $x + y = m$ from the origin $m/\sqrt{2}$. Since the line cuts the ellipse we must have

$$\frac{m}{\sqrt{2}} \leq \sqrt{\frac{2n}{m}} \quad \Rightarrow \quad m \leq 2^{\frac{2}{3}} n^{\frac{1}{3}} \quad (2).$$

By (1) and (2)

$$n^{\frac{1}{3}} \leq m \leq 2^{\frac{2}{3}} n^{\frac{1}{3}}.$$

(2a) Substitute $v = m - u$ in $n/m = u^2 - uv + v^2$ to obtain the equation

$$\frac{n}{m} = 3(u^2 - mu) + m^2.$$

Hence $3 \mid m^2 - n/m$. Since, by (1a) $n \leq m^3$, $l = (m^2 - n/m)/3 \geq 0$.

(3a) Now consider the value of l: $l = -u^2 + mu$. This means u is an integer root of the quadratic equation $x^2 - mx + l = 0$ with integer coefficients, so the discriminant, namely $m^2 - 4l$, must be a perfect square.

(1b) If $u \geq 0$ and $v < 0$ then the point (u, v) lies on E in the fourth quadrant so the line $m = x + y$ cuts the x-axis to the left of $x = \sqrt{n/m}$ leading to the bound $m < n^{1/3}$. The proofs of (2b) and (3b) are similar to those of (2a) and (3a).

Now assume that (1a-3a) are satisfied. (The case (1b-3b) is similar.)

Given m, from (1a) define l using (1b) so $3l = m^2 - n/m$. Let x_1, x_2 be the two integer roots (given by condition (1c) of the quadratic equation

$$x^2 - mx + l = 0$$

so $x_1 x_2 = l$, the product of the roots, and $m = x_1 + x_2$, the sum of the roots.

Then

$$\begin{aligned} n &= m \cdot \frac{n}{m} \\ &= (x_1 + x_2)(m^2 - 3l) \\ &= (x_1 + x_2)((x_1 + x_2)^2 - 3x_1x_2) \\ &= (x_1 + x^2)(x_1^2 - x_1x_2 + x_2^2) \\ &= x_1^3 + x_2^3. \end{aligned}$$

3 Modular Constraints

By analogy with the sum of two squares it is natural to consider modular conditions on n for it to be representable as the sum of two cubes. Something interesting is happening here when the modulus is divisible by 7 or 9:

Example 1. Let $n \in \mathbb{N}$ be such that n satisfies one of the congruences listed below. Then $n = x^3 + y^3$ has no solution in $\mathbb{Z}$:

1. $n \equiv 3 \text{ or } 4 \mod 7$,
2. $n \equiv 3, 4, 5 \text{ or } 6 \mod 9$,
3. $n \equiv 3, 4, 5, 6, 10, 11, 12, 13, 14, 15, 17, 18, 21,$
$22, 23, 24, 25, 30, 31, 32, 33, 38, 39, 40,$
$41, 42, 45, 46, 48, 49, 50, 51, 52, 53, 57,$
$58, 59, \text{ or } 60 \mod 63$.

Theorem 2. *Let m, n be such that there exist u, v, x, y with*

$$\begin{aligned} m &\equiv u^3 + v^3 \mod 7 \\ n &\equiv x^3 + y^3 \mod 9. \end{aligned}$$

Then there exist integers A, B such that

$$28m - 27n \equiv A^3 + B^3 \mod 63.$$

Furthermore, every sum of two cubes modulo 63 arises in this manner.

Proof. Let $A = 28u - 27x$ and $B = 28v - 27y$ and expand $A^3 + B^3$ modulo 63 to derive the given equation. A computation verifies the last claim of the theorem statement.

If $N \geq 2$ let

$$\delta(N) = \frac{\#\{n \in \{1, \ldots, N\} : n \equiv x^3 + y^3 \bmod N \text{ has a solution}\}}{N}.$$

Lemma 1. *Let $n \in \mathbb{Z}$ be given and p be a prime with $p \neq 3$. Then if the equation $n \equiv x^3 + y^3 \bmod p$ has a solution so also does the equation $n \equiv x^3 + y^3 \bmod p^\alpha$ for every $\alpha \geq 1$.*

Proof. Let $n \equiv x^3 + y^3 \bmod p$. Assume that $p \nmid x$. (If $p \mid x$ and $p \mid y$ then $p \mid n$, so we can use $x = 1$ and $y = -1$.) Assume, using induction, that $n \equiv x^3 + y^3 \bmod p^\alpha$ has a solution for some $\alpha \geq 1$ with $p \nmid x$. Then

$$x^3 + y^3 - n = lp^\alpha$$

for some $l \in \mathbb{Z}$ and so, if m is an integer to be chosen later,

$$\begin{aligned}(x + mp^\alpha)^3 = y^3 - n &\equiv x^3 + y^3 - n + 3mx^2p^\alpha \bmod p^{\alpha+1} \\ &\equiv p^\alpha(l + 3mx^2) \bmod p^{\alpha+1}.\end{aligned}$$

But $p \neq 3$ and $p \nmid x$ so we can choose m with $l + 3mx^2 \equiv 0 \bmod p$ giving

$$n \equiv (x + mp^\alpha)^3 + y^3 \bmod p^{\alpha+1}$$

and $p \nmid x + mp^\alpha$ since $p \nmid x$. This completes the inductive step.

Lemma 2. *Let $n \in \mathbb{Z}$ be given. Then if the equation $n \equiv x^3 + y^3 \bmod 3^2$ has a solution so also does the equation $n \equiv x^3 + y^3 \bmod 3^\alpha$ for every $\alpha \geq 2$.*

Proof. Let $n \equiv x^3 + y^3 \bmod 3^2$. Assume that $3 \nmid x$. (If $3 \mid x$ and $3 \mid y$ then $3^2 \mid n$, so we can use $x = 1$ and $y = -1$.) Assume that $n \equiv x^3 + y^3 \bmod 3^\alpha$ has a solution for some $\alpha \geq 2$ with $3 \nmid x$. Then

$$x^3 + y^3 - n = l3^\alpha$$

for some $l \in \mathbb{Z}$ and so, if m is an integer to be chosen later,

$$\begin{aligned}(x + m3^{\alpha-1})^3 = y^3 - n &\equiv x^3 + y^3 - n + mx^2 3^\alpha \bmod 3^{\alpha+1} \\ &\equiv 3^\alpha(l + mx^2) \bmod 3^{\alpha+1}.\end{aligned}$$

Choose m with $l + mx^2 \equiv 0 \bmod 3$ giving

$$n \equiv (x + m3^{\alpha-1})^3 + y^3 \bmod 3^{\alpha+1}.$$

Theorem 3. *The positive integer m is such that $7 \nmid m$ and $9 \nmid m$ if and only if $\delta(m) = 1$. If $7 \mid m$ and $9 \nmid m$ then $\delta(m) = 5/7$. If $9 \mid m$ and $7 \nmid m$ then $\delta(m) = 5/9$. If $7 \mid m$ and $9 \mid m$ then $\delta(m) = 25/63$.*

Proof. The "if" direction follows directly from the example at the start of this section, so assume m is such that $7 \nmid m$ and $9 \nmid m$.

By [9], $\delta(p) = 1$ for $p \neq 2, 3, 7$. Simple computations lead to the values $\delta(2) = 1, \delta(3) = 1, \delta(9) = 5/9$, $\delta(7) = 5/7$.

By the Chinese remainder theorem and the definition of addition and multiplication in a product ring, if $(N, M) = 1$, then $\delta(MN) = \delta(M)\delta(N)$. Hence we need only consider values of m which are prime powers.

By Lemma 1, if $p \neq 3$, $\delta(p^\alpha) = \delta(p)$ for all $\alpha \geq 1$. By Lemma 2, $\delta(3^\alpha) = \delta(9)$ for all $\alpha \geq 2$ and the theorem follows directly.

4 The Functions Theta and Eta

Definition 1. *Let $n \in \mathbb{N}$. Then $\theta(n)$ is the least positive integer such that the Diophantine equation*

$$n\theta(n) = x^3 + y^3$$

has a solution with $x \geq 0$ and $y \geq 0$.

Because

$$(n+1)^3 + (n-1)^3 = 2n(n^2+3)$$

the function θ is well defined and $\theta(n) \leq 2(n^2+3)$. The positive integer n is expressible as the sum of two positive cubes if and only if $\theta(n) = 1$.

Sometimes a distinction is made between general solutions to equations like $n = x^3 + y^3$ and the narrower class of so called "proper" or "primitive" solutions, namely those with x and y having no common factors, $(x, y) = 1$. This is to exclude the solutions $ab^3 = (xb)^3 + (yb)^3$, given the representation $a = x^3 + y^3$.

Definition 2. *Let $n \in \mathbb{N}$. Then $\eta(n)$ is the least positive integer such that the Diophantine equation*

$$n\eta(n) = x^3 + y^3$$

has a solution with $x \geq 0$ and $y \geq 0$ and $(x, y) = 1$.

Because

$$(n+1)^3 + (n-1)^3 = 2n(n^2+3)$$

and satisfies $(n+1, n-1) = 1$ if n is even, and

$$(\frac{n+1}{2})^3 + (\frac{n-1}{2})^3 = n(\frac{n^2+3}{4})$$

satisfies $(\frac{n+1}{2}, \frac{n-1}{2}) = 1$ if n is odd, the function η is well defined and $\eta(n) = O(n^2)$ also. The positive integer n is expressible as the sum of two positive cubes which are coprime if and only if $\eta(n) = 1$. Clearly $\theta(n) \leq \eta(n)$ for all $n \in \mathbb{N}$.

Theorem 4. *The composite function values $\theta \circ \theta$ and $\eta \circ \eta$ satisfy $\theta^2(n) \leq n$ and $\eta^2(n) \leq n$ for all $n \in \mathbb{N}$.*

Proof. By the definition of θ applied to $\theta(n)$, there exist x, y such that $\theta^2(n) \cdot \theta(n) = x^3 + y^3$ and $\theta^2(n)$ is the smallest multiple of $\theta(n)$ which can be expressed as the sum of two cubes. But $n \cdot \theta(n) = u^3 + v^3$ for some u, v also. Therefore $\theta^2(n) \leq n$. The proof for η is similar.

Theorem 5. *For each $n \in \mathbb{N}$ the sequences $(\theta^j(n))$ and $(\eta^j(n))$ are either constant after a finite number of terms or periodic with period 2.*

Proof. Since for all $n \in \mathbb{N}$, $n \geq \theta^2(n) \geq 1$, the sequence of values $(\theta^j(n)$ is eventually periodic. Assume the length of the period is $n \geq 3$. Then there exist distinct integers $a_1, \cdots, a_n$ with

$$\theta(a_1) = a_2, \theta(a_2) = a_3, \cdots, \theta(a_{n-1} = a_n, \theta(a_n) = a_1.$$

If n is even $a_1 \geq a_3 \geq a_5, \cdots \geq a_{n-1} \geq a_1$ so $a_1 = a_3$ which is false. If n is odd we cycle through twice:

$$a_1 \geq a_3 \geq \cdots a_n \geq a_2 \geq \cdots \geq a_1,$$

so again $a_1 = a_3$. Hence the length of the period n must be one or two. The proof for η is similar.

Note that if (x, y) is the closest integral point on $n = x^2 - xy + y^2$ to the line $y = -x$ and such that $x + y > 0$ then $\theta(n) \leq x + y$. Another problem is to characterize those n such that $\theta(n) = x + y$, this minimum positive value.

Note also that a function like θ can be defined for forms with appropriate symmetry properties, e.g. $f(x, y) = x^k + y^k$ for k odd.

Acknowledgements: The support of the Department of Mathematics of the University of Waikato, the discussions held with Ian Hawthorn and the valuable contributions, especially to shortening the proof of Theorem 3, of an anonymous referee are warmly acknowledged.

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer Verlag, 1976.
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford, 1979.
3. K. L. Hua, *Introduction to Number Theory*, Springer-Verlag, 1982.
4. S. Lang, Old and new conjectured diophantine inequalities, *Bull. Amer. Math. Soc.*, **23**, (1990), 37–75.
5. L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
6. M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Springer-Verlag, 1996.
7. M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, 1996.
8. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.
9. A. G. Vosper, The critical pairs of subsets of a group of prime order. *J. London Math. Soc.*, **31**, (1956), 200–205, 280–282.