

A Computational Approach to Characterizing the Sum of Two Cubes

Kevin A. Broughan

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

Abstract. A computational approach to finding an intrinsic characterization of integers which are cube free and can be expressed as the sum of two cubes, $n = x^3 + y^3$, is developed. Every n has a multiple which is a sum of two cubes. A function $\theta(n)$ is defined to model this phenomena and is found to be periodic. Testing modulo 7 and modulo 9 is optimal for modular conditions. A divisibility test requires detailed knowledge of the positions of integer points on the quadratic curve $m = x^2 - xy + y^2$. These test reduce the number of potential sums of cubes by a factor of 10, when restricted to cube free numbers, but this is still 4 times the exact number of sums of cubes. A discussion of the conjecture that $x^n + y^n = 2z^n, n \geq 3, (x, y) = 1, x \geq 0, y \geq 0$ implies $x = y = z = 1$ is included.

1 Introduction

The beautiful characterization of numbers which are the sum of two squares is not matched by any 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 [4], [5].

In this paper a computational approach is adopted to the question of determining when a given integer n can be expressed as the sum of two cubes. This is really not an algorithmic problem, since a direct search through all sums of cubes up to n leads to a test of complexity $O(n^{2/3})$. Here we are looking for some intrinsic characterization, some property of n itself which will determine whether it is representable or not.

Needless to say the approach adopted here only goes part of the distance towards the stated goal. It is also restricted to numbers which are cube-free: this simplification of the task makes any representation automatically primitive.

In Section Two there are lemmas and a theorem giving the divisor sum of a multiplicative function with values in $\{-1, 0, 1\}$. In Section Three the quadratic form $n = x^2 - xy + y^2$ is studied with a particular emphasis on values of n for which it has points with integer coordinates and, if so, where those points lie on the curve. In Section Four a function representing the least multiplier of n , so that the multiple may be represented as the sum of two cubes, is defined. It is proved to be eventually constant or periodic with period two. Section Five considers the equation $n = x^3 + y^3$ modulo m . It is shown that the divisibility

of m by 7 or 9 is interesting, in that it is in these cases (and conjecturally only these) the form $n \equiv x^3 + y^3 \pmod{m}$ does not have a solution for every n . In Section Six the factors $n = a \cdot b$ are examined and some inequality constraints are developed, based on $a = x + y, b = x^2 - xy + y^2$ and the work in Section Three. Then the tests are applied sequentially to the cube free numbers up to 100, 1000, 10000 and 100000 respectively, and compared with the exact number of representable numbers in these ranges.

In an end note the conjecture that $x^n + y^n = 2z^n, n \geq 3, (x, y) = 1$ implies $x = y = z = 1$ is discussed. The conjecture may be shown to be true, for n sufficiently large, if the ABC conjecture is assumed.

All algorithms used were encoded in Mathematica or Common Lisp.

2 Preliminary Lemmas

Lemma 1. *If $n \in \mathbb{N}$ is cube free and $n = x^3 + y^3$, then $(x, y) = 1$.*

Proof. If $(x, y) = d$ and $n = x^3 + y^3$ then $d^3 \mid n$ so $d = 1$.

Lemma 2. *If $(x, y) = 1$ and $n = x^3 + y^3$ then $(x + y, x^2 - xy + y^2) = (x + y, 3)$.*

Proof.

$$\begin{aligned} (x + y, x^2 - xy + y^2) &= (x + y, y^2 - 2xy) \\ &= (x + y, -3xy) \\ &= (x + y, 3) \text{ since } (x, y) = 1 \end{aligned}$$

Lemma 3. *If $n = x^3 + y^3$ in integers with $(x, y) = 1$, then $3 \mid n$ implies $9 \mid n$.*

Proof. Let $a = x + y, b = x^2 - xy + y^2$, so $n = ab$ and $3(x^2 - ax) + a^2 = b$. Therefore $3 \mid a$ if and only if $3 \mid b$.

Theorem 1. *Let $f : \mathbb{Z} \rightarrow \{-1, 0, 1\}$ be completely multiplicative. Then, for all $n \in \mathbb{N}$, $\sum_{d \mid n} f(d) = 0$ if and only if there is a prime p with $p^\alpha \parallel n$ and α odd, such that $f(p) = -1$.*

Otherwise,

$$\sum_{d \mid n} f(d) = \prod_{p^\alpha \parallel n, f(p)=1} (1 + \alpha),$$

where there is one term in the product on the right hand side for each prime p dividing n with $f(p) = 1$.

Proof. Let $\eta \in (0, 1)$ and let $n \in \mathbb{N}$ have its standard prime factorization

$$n = \prod_{j=1}^m p_j^{\alpha_j}.$$

For $1 \leq j \leq m$ let x_j be real numbers with $x_j \neq 1$ for all j . Let $\alpha_j \in \mathbb{N}$. Then

$$\sum_{0 \leq i_j \leq \alpha_j} \prod_{j=1}^m x_j^{i_j} = \prod_{j=1}^m \frac{1 - x_j^{\alpha_j+1}}{1 - x_j}.$$

For each j let $x_j = f(p_j)$. Then

$$\sum_{0 \leq i_j \leq \alpha_j} \prod_{j=1}^m \eta^{i_j} (f(p_j)^{i_j}) = \prod_{j=1}^m \frac{1 - \eta^{\alpha_j+1} f(p_j)^{\alpha_j+1}}{1 - \eta f(p_j)}.$$

Abbreviate each term in this product by $F(\eta, j)$.

Now let $\eta \rightarrow 1^-$. The sum on the left hand side tends to

$$\sum_{0 \leq i_j \leq \alpha_j} f\left(\prod_{j=1}^m p_j^{i_j}\right) = \sum_{d|n} f(d).$$

Divide the product on the right up into four terms,

$$\{1, \dots, m\} = Z \cup P \cup E \cup D$$

where

$$\begin{aligned} Z &= \{j : f(p_j) = 0\}, \\ P &= \{j : f(p_j) = 1\}, \\ E &= \{j : f(p_j) = -1 \text{ and } \alpha_j \text{ is odd}\}, \\ D &= \{j : f(p_j) = -1 \text{ and } \alpha_j \text{ is even}\}. \end{aligned}$$

Then

$$\lim_{\eta \rightarrow 1^-} \prod_{j \in Z} F(\eta, j) = 1,$$

and

$$\lim_{\eta \rightarrow 1^-} \prod_{j \in P} F(\eta, j) = \lim_{\eta \rightarrow 1^-} \prod_{j \in P} \frac{1 - \eta^{\alpha_j+1}}{1 - \eta} = \prod_{j \in P} (\alpha_j + 1),$$

and

$$\lim_{\eta \rightarrow 1^-} \prod_{j \in E} F(\eta, j) = \lim_{\eta \rightarrow 1^-} \prod_{j \in P} \frac{1 + \eta^{\alpha_j+1}}{1 + \eta} = 1,$$

and, if $D = \emptyset$

$$\lim_{\eta \rightarrow 1^-} \prod_{j \in D} F(\eta, j) = 1,$$

whereas if D is not empty,

$$\lim_{\eta \rightarrow 1^-} \prod_{j \in D} F(\eta, j) = 0.$$

The theorem now follows directly from these derivations.

Corollary 1. *Let D be an integer, congruent to 0 or 1 modulo 4 and not a square, and, for each $n \in \mathbb{N}$, let $(D | n)$ be Kronecker's extension of the Legendre symbol [1] (as defined below). Then*

$$\sum_{d|n} (D | n) = 0$$

if and only if there exists an odd prime p and odd α with $p^\alpha \parallel n$ and with D not a quadratic residue mod p , or an odd α with $2^\alpha \parallel n$ and $D \equiv 5 \pmod{8}$.

Definition 1. *Kronecker's symbol $(D | n)$ is defined, for D with the same restrictions as in the above corollary, as follows: Let $(D | 1) = 1$. If $4 \mid D$, let $(D | 2) = 0$, if $D \equiv 1 \pmod{8}$ let $(D | 2) = 1$ and if $D \equiv 5 \pmod{8}$ let $(D | 2) = -1$. If p is an odd prime, then the value of $(D | p)$ is the same as that of the Legendre symbol $(D | p)$. If $n \in \mathbb{N}$ is not prime, then let*

$$(D | n) = \prod_{j=1}^m (D | p_j)^{\alpha_j}$$

where

$$n = \prod_{j=1}^m p_j^{\alpha_j}$$

is the standard factorization.

Corollary 2. *Let $\lambda : \mathbb{N} \rightarrow \{-1, 1\}$ be Liouville's function. Then for $n \in \mathbb{N}$, $\sum_{d|n} \lambda(n) = 0$ if and only if there exists a prime p and odd α such that $p^\alpha \parallel n$.*

Corollary 3. *Let $\chi : \mathbb{Z} \rightarrow \{-1, 0, 1\}$ be a real, non-principle Dirichlet character [1]. Then for $n \in \mathbb{N}$,*

$$\sum_{d|n} \chi(n) = 0$$

if and only if there is a prime p and odd α with $p^\alpha \parallel n$ and such that $\chi(p) = -1$.

3 Values of a Quadratic Form

Definition 2. *We say a divides b oddly if the maximum power of a which divides b is an odd power.*

Theorem 2. *Let $n \in \mathbb{N}$. Then $n = x^2 - xy + y^2$ has a solution in \mathbb{Z} with $(x, y) = 1$ only if $9 \nmid n$ and every prime $p \neq 3$ dividing n satisfies $p \equiv 1 \pmod{3}$.*

Proof. 1. If $3^2 \mid n$, then $36m = (2x - y)^2 + 3y^2$ for some m so $3 \mid y$ and $3 \mid 2x - y$ contradicting $(x, y) = 1$.

2. The form $x^2 - xy + y^2$ is odd except when both x and y are even, which is impossible if $(x, y) = 1$. More generally:

3. Let $p \neq 3$ divide $x^2 - xy + y^2$. Then $p \nmid x$ and $p \nmid y$. Since $p \mid (2x - y)^2 + 3y^2$ and $(y, p) = 1$, -3 is a quadratic residue mod p , so therefore $p \equiv 1 \pmod{3}$.

The converse of this theorem is also true. An algorithm to check the converse for values $1 \leq x, y \leq N$ is the following: take the complement of all admissible values of n , and then check, for each such n , whether $9 \mid n$ or whether n has a prime divisor $p \neq 3$ with $p \equiv 2 \pmod{3}$. The complexity is $O(N^2)$.

In the figure below the points with integer coordinates on the curve $n = x^2 - xy + y^2$ are marked for a given value of $n = 7 \cdot 13^2 = 1183$. The coordinates of these points are given for reference:

{48, 25}, {48, 23}, {47, 32}, {47, 15}, {45, 37}, {45, 8},
 {43, 40}, {43, 3}, {40, 43}, {40, -3}, {37, 45}, {37, -8},
 {32, 47}, {32, -15}, {25, 48}, {25, -23}, {23, 48}, {23, -25},
 {15, 47}, {15, -32}, {8, 45}, {8, -37}, {3, 43}, {3, -40},
 {-3, 40}, {-3, -43}, {-8, 37}, {-8, -45}, {-15, 32}, {-15, -47},
 {-23, 25}, {-23, -48}, {-25, 23}, {-25, -48}, {-32, 15},
 {-32, -47}, {-37, 8}, {-37, -45}, {-40, 3}, {-40, -43},
 {-43, -3}, {-43, -40}, {-45, -8}, {-45, -37},
 {-47, -15}, {-47, -32}, {-48, -23}, {-48, -25}}

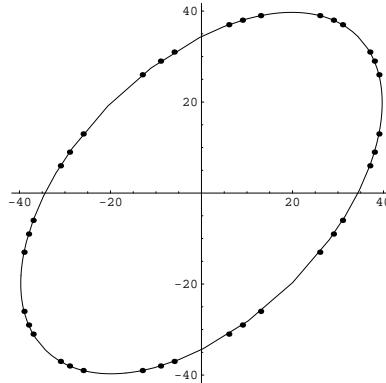


Fig. 1. Integer points on $n = x^2 - xy + y^2$ with $n = 7 \cdot 13^2$

These points have been computed simply by fixing n and then computing the value of the quadratic form for all integral values (x, y) in the range $0 < x < \sqrt{n/3}, \sqrt{n} < y < 2\sqrt{n/3}$, (see Theorem 6.1 below), and checking to see which points are on the curve.

Theorem 3. *Let $n = x^2 - xy + y^2$ be the equation of an ellipse in the real plane and let $s(n) = \sum_{d|n} (-3|d)$. Then there are $s(n)$ points with integer coordinates on the ellipse in each of the second and fourth quadrants, and in each of the two symmetric sectors dividing the first and third sectors.*

Proof. The correspondence $(x, y) \rightarrow (-x, -y)$ shows there are the same number of points in the second and fourth quadrants. Similarly, the correspondence

$(x, y) \rightarrow (y, x)$ shows the same is true for the two symmetric sectors dividing the first and third quadrants. Finally the mapping $(x, y) \rightarrow (y - x, y)$ shows there are the same number of points on the curve in the second quadrant and each part of the first quadrant.

4 The Functions Theta and Eta

Definition 3. 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 $\theta(n) = O(n^2)$. The positive integer n is expressible as the sum of two positive cubes if and only if $\theta(n) = 1$.

Definition 4. 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

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

satisfies $\left(\frac{n+1}{2}, \frac{n-1}{2}\right) = 1$ 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 $n \in \mathbb{N}$.

Example 1. Mathematica code for computing the value of $\theta(n)$ is as follows:

```
theta[n_] := Module[{k = 1},
  While[Not[theta[n, k]], k = k + 1];
  Return[k]

theta[n_, k_] := Module[{cuberoot = N[(k n)^(1/3)], ans = False},
  Do[If[i^3 + j^3 == k n, {ans = True, Break[]}],
    {i, 1, cuberoot}, {j, i, cuberoot}];
  Return[ans]]
```

The 14 sequences of values $(\theta^j(n) : j \geq 0)$ with $1 \leq n \leq 14$ are given below:

$\{1, 2, 1\}, \{2, 1, 2\}, \{3, 3\}, \{4, 4\}, \{5, 7, 4, 4\}, \{6, 9, 1, 2, 1\}, \{7, 4, 4\}, \{8, 2, 1, 2\}, \{9, 1, 2, 1\}, \{10, 25, 10\}, \{11, 31, 7, 4, 4\}, \{12, 6, 9, 1, 2, 1\}, \{13, 5, 7, 4, 4\}, \{14, 2, 1, 2\}.$

Similarly, the sequences $(\eta^j(n) : j \geq 0)$ with $1 \leq n \leq 14$ are given also:

$\{1, 2, 1\}, \{2, 1, 2\}, \{3, 3\}, \{4, 7, 4\}, \{5, 7, 4, 7\}, \{6, 21, 6\}, \{7, 4, 7\}, \{8, 19, 7, 4, 7\}, \{9, 1, 2, 1\}, \{10, 37, 10\}, \{11, 31, 7, 4, 7\}, \{12, 39, 9, 1, 2, 1\}, \{13, 5, 7, 4, 7\}, \{14, 2, 1, 2\}.$

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, \dots, a_n with

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

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

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

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

Example 2. The following terminal values for θ have been computed: period 1: $\{3, 4\}$ and period 2: $\{1, 2\}$ and $\{10, 25\}$. For η period 1: $\{3\}$ and period 2: $\{1, 2\}, \{4, 7\}, \{6, 21\}$ and $\{10, 37\}$.

An interesting problem would be to characterize the whole numbers n such that $\theta(n) = \eta(n)$ or $\theta(n) = n$, or pairs $n \neq m$ such that $\eta(n) = m, \eta(m) = n$.

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.

5 Modular Constraints

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

The following theorem is a direct consequence of items 1 and 2 in the list above:

Theorem 6. *Let $m \geq 2$ be an integer. If for every n there is a solution x, y to the congruence*

$$n \equiv x^3 + y^3 \pmod{m}$$

then $7 \nmid m$ and $9 \nmid m$.

Example 4. It is strongly suspected that the converse of this theorem is also true. A direct computation shows that if $2 \leq m \leq 1200$ then

$$n \equiv x^3 + y^3 \pmod{m}$$

has no solution \pmod{m} , for some values of $n \in \mathbb{N}$, if m is divisible by 7 or 9. Note that it follows from a theorem of Vosper [6] that if $p \geq 13$ and $p \equiv 1 \pmod{3}$ then the congruence $n \equiv x^3 + y^3 \pmod{p}$ has a solution for every n . (The same is true for every prime p if the number of cubes is increased to 3.)

It has also been shown that, by a straight forward computation, that for a smaller range of moduli m , the proportion of values of n where there is a solution is $\frac{5}{7}$ if $7 \mid n$ and $9 \nmid n$, $\frac{5}{9}$ if $7 \nmid n$ and $9 \mid n$ and $\frac{25}{63}$ if $63 \mid n$.

Theorem 7. *Let m, n be such that there exist u, v, x, y with*

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

Then there exist integers A, B such that

$$28m - 27n \equiv A^3 + B^3 \pmod{63}.$$

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

Proof. Let $A = 28u - 27v$ 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.

6 Inequality Constraints and Example Computations

Theorem 8. *Let $n \in \mathbb{N}$ be such that the Diophantine equation $n = x^2 - xy + y^2$ has integral solutions. Then there exists a solution (x_o, y_o) with $0 \leq x_o \leq \sqrt{n/3}$ and $\sqrt{n} \leq y_o \leq 2\sqrt{n/3}$. If (x_o, y_o) is any positive solution, then $x_o + y_o \leq 2\sqrt{n}$.*

Proof. By Theorem 3.2 above and some simple geometry, there is a solution (x, y) with $0 \leq x_o \leq \sqrt{n}$ and $\sqrt{n} \leq y_o \leq 2\sqrt{n/3}$. But if $x > \sqrt{n/3}$ then $(y - x, y)$ is a solution satisfying the statement of the theorem. The final conclusion also follows from some simple geometry.

Definition 5. *We say n passes the modular test if $n \equiv 0, 1, 2, 5$ or $6 \pmod{7}$ and $n \equiv 0, 1, 2, 7$ or $8 \pmod{9}$.*

Definition 6. *We say n passes the divisor test if there exists a factorization $n = ab$ with, $b \leq \sqrt{3n}$ and $a \leq \sqrt{b}$ and such that for all $p \mid b$ with $p \neq 3$, $p \equiv 1 \pmod{3}$.*

Example 5. In the table below, for each of the given values of N , the number of cube free numbers less than or equal to N is listed, then the number of these which are congruent to an admissible value modulo 9, then the number of these congruent to an admissible value modulo 7, then then number of these which pass the divisor test described above. In the final row the exact number of sums of positive cubes, which are cube free and less than or equal to N , is given.

N	100	1000	10000	100000
cube free	85	833	8319	83190
Mod 9 test	46	449	4480	44795
Mod 7 test	34	317	3196	31961
Divisor test	12	82	818	8115
Exact number	6	21	101	477

Considering the numbers up to 100, those expressible as primitive sums of cubes, under the requirements of this study are:

{2, 9, 28, 35, 65, 91}.

Those remaining after the application of the tests are:

{1, 2, 9, 28, 35, 36, 63, 65, 70, 90, 91, 99}.

By using the facts (1) when $(x, y) = 1$, $x^2 - xy + y^2$ is odd, (2) when $3 \mid x + y$ then $3 \mid x^2 - xy + y^2$, (3) $9 \nmid x^2 - xy + y^2$ and (4) if $3 \nmid x + y$ then $(x + y, x^2 - xy + y^2) = 1$, together with (5) the inequality constraints implied by the divisor test, each of the remaining numbers {36, 63, 70, 90, 99} has been shown (individually, by hand) to be inexpressible as the sum of two coprime positive cubes. The algorithmic content of these deductions has yet to be extracted.

7 Endnote

Somewhat loosely related to this study, but included because they also lend themselves to computational and algorithmic exploration, are generalizations of the Diophantine equation $x^3 + y^3 = 2z^3$. Mordell [3] has shown, using the field $\mathbb{Q}(\rho)$ where ρ is a complex cube root of unity, that the only positive solution of this equation with $(x, y) = 1$ is $x = y = z = 1$. (Note that the equation $x^2 + y^2 = 2z^2$ has an infinite family of solutions with $(x, y) = 1$ namely

$$\begin{aligned}x &= a^2 - b^2 + 2ab \\y &= a^2 - b^2 - 2ab \\z &= a^2 + b^2\end{aligned}$$

where a and b are integers with $(a, b) = 1$.)

Conjecture 1. Let $n > 2$ be given. Then the equation $x^n + y^n = 2z^n$ has no solution in \mathbb{Z} other than $x = y = z = 1$. (Assuming the truth of the ABC conjecture [2], there is an n_o such that this is true for $n \geq n_o$.)

Acknowledgements: The support of the Department of Mathematics of the University of Waikato and the valuable discussions held with Ian Hawthorn are warmly acknowledged.

References

1. Apostol, T.M.: Introduction to Analytic Number Theory. New York, Berlin Heidelberg: Springer Verlag, 1976.
2. Lang, S.: Old and new conjectured diophantine inequalities. Bull. Amer. Math. Soc **23**, (1990), 37-75.
3. Mordell, L.J.: Diophantine Equations. London, New York: Academic Press, 1969.
4. Nathanson, M.B.: Additive Number Theory, The Classical Bases. New York, Berlin, Heidelberg: Springer-Verlag, 1996.
5. Silverman, J. H. and Tate, J.: Rational Points on Elliptic Curves. New York, Berlin, Heidelberg: Springer-Verlag, 1992.
6. Vosper, A.G.: The critical pairs of subsets of a group of prime order. J. London Math. Soc., **31**, (1956), 200-205, 280-282.