Journal of Integer Sequences, Vol. 18 (2015),
Article 15.8.6

# Representation of Integers Using $a^2 + b^2 - dc^2$

Peter Cho-Ho Lam
Department of Mathematics
Simon Fraser University
Burnaby, BC V5A1S6
Canada
chohol@sfu.ca

**Abstract**

A positive integer $d$ is called *special* if every integer $m$ can be expressed as $a^2 + b^2 - dc^2$ for some nonzero integers $a, b, c$. A necessary condition for special numbers was recently given by Nowicki, and in this paper we prove its sufficiency. Thus, we give a complete characterization for special numbers.

## 1 Introduction

Many problems in number theory are concerned with the representation of integers by multivariate polynomials with integral coefficients and variables. For example, the well-known theorem of Lagrange asserts that every positive integer is the sum of four squares. Ramanujan [3] gave a complete list of general quadratic forms with four variables,

$$Q(x, y, z, w) = ax^2 + by^2 + cz^2 + dw^2,$$

that represent all positive integers, where $a, b, c, d \in \mathbb{N}$. Note that it is not possible to represent all positive integers if we reduce one variable in $Q(x, y, z, w)$; in fact, it cannot even represent all integers from 1 to 10 by a very elementary argument. However, three variables are sufficient if we use indefinite quadratic forms. For example, the form $Q(x, y, z) = x^2 + y^2 - z^2$ can represent all integers with integral $x, y, z$ since $x^2 - z^2$ represents all odd integers and one can pick $y = 0, 1$. To generalize this, Nowicki [2] defined special numbers and proved a necessary condition for them, which is stated in Theorem 2:

**Definition 1.** A positive integer $d$ is *special* if for every integer $m$ there exist nonzero integers $a, b, c$ such that $m = a^2 + b^2 - dc^2$.

**Theorem 2.** *Every special number $d$ is of the form $q$ or $2q$, where either $q = 1$ or $q$ is a product of primes of the form $4m + 1$.*

Nowicki [2] further verified that the converse is true when $d \leq 50$ through various identities. For example, when $d = 13$, we have

$$(2k-4)^2 + (3k-10)^2 - 13(k-3)^2 = (2k-30)^2 + (3k-36)^2 - 13(k-13)^2 = 2k-1,$$
$$(2k-3)^2 + (3k-2)^2 - 13(k-1)^2 = (2k-29)^2 + (3k-54)^2 - 13(k-17)^2 = 2k.$$

We need two identities for each parity since we require $a, b, c$ to be nonzero. Similarly, when $d = 34$, we have

$$(3k-7)^2 + (5k-16)^2 - 34(k-3)^2 = (3k-24)^2 + (5k-33)^2 - 34(k-7)^2 = 2k-1,$$
$$(3k-11)^2 + (5k-27)^2 - 34(k-5)^2 = (3k-45)^2 + (5k-61)^2 - 34(k-13)^2 = 4k,$$
$$(3k-1)^2 + (5k+1)^2 - 34(k)^2 = (3k-69)^2 + (5k-135)^2 - 34(k-26)^2 = 4k+2.$$

In this paper, we prove the converse of Theorem 2, and hence give a complete characterization of special numbers:

**Theorem 3.** *If $d$ is of the form $q$ or $2q$, where either $q = 1$ or $q$ is a product of primes of the form $4m + 1$, then $d$ is special.*

## 2 Proof of Theorem 3

First, we invoke the following well-known lemma, where the proof is given in [1, Theorem 3.20]:

**Lemma 4.** *A positive integer $n$ can be expressed as the form $q$ or $2q$ where $q$ is a product of primes of the form $4m + 1$ if and only if $n$ can be expressed as the form $n = x^2 + y^2$ where $x, y \in \mathbb{N}$ and $\gcd(x, y) = 1$.*

*Proof of Theorem 3.* In what follows, we assume $d > 1$, since $d = 1$ is already known to be special.

Suppose $d$ is odd. Then all prime factors of $d$ are of the form $4m + 1$. By Lemma 4, we can write $d = x^2 + y^2$ where $\gcd(x, y) = 1$, and $x \not\equiv y \pmod 2$. Now let $a = xk + \alpha, b = yk + \beta$ and $c = k$, where $\alpha$ and $\beta$ are integers which will be chosen later. It follows that

$$\begin{aligned} a^2 + b^2 - dc^2 &= (xk+\alpha)^2 + (yk+\beta)^2 - (x^2+y^2)(k)^2 \\ &= 2(x\alpha + y\beta)k + \alpha^2 + \beta^2. \end{aligned} \tag{1}$$

We consider the solution pairs $(\alpha, \beta)$ to the equation

$$x\alpha + y\beta = 1. \tag{2}$$

It suffices to show that $\alpha^2+\beta^2$ cover both parities. Note that (2) must have an integral solution $(\alpha_0, \beta_0)$ since $\gcd(x, y) = 1$. If we define $\alpha_1 = \alpha_0 + y$ and $\beta_1 = \beta_0 - x$, then $(\alpha_1, \beta_1)$ is another solution of (2). Now observe

$$\begin{aligned}
\alpha_1^2 + \beta_1^2 &= (\alpha_0 + y)^2 + (\beta_0 - x)^2 \\
&= (\alpha_0^2 + \beta_0^2) + x^2 + y^2 + 2(\alpha_0 y + \beta_0 x) \\
&\equiv (\alpha_0^2 + \beta_0^2) + x^2 + y^2 \pmod 2.
\end{aligned}$$

Since $x^2 + y^2 = d$ is odd, $\alpha_0^2 + \beta_0^2 \not\equiv \alpha_1^2 + \beta_1^2 \pmod 2$. The two identities given by

$$(xk + \alpha_i)^2 + (yk + \beta_i)^2 - (x^2 + y^2)(k)^2 = 2k + \alpha_i^2 + \beta_i^2,$$

where $i = 0, 1$, cover both odd and even integers, and hence every integer can be expressed as the form $a^2 + b^2 - dc^2$ for some integers $a, b, c$.

However, one of the variables $a, b, c$ becomes zero in the representations of

$$m = \alpha_i^2 + \beta_i^2, -\frac{2\alpha_i}{x} + \alpha_i^2 + \beta_i^2, -\frac{2\beta_i}{y} + \alpha_i^2 + \beta_i^2 \tag{3}$$

for $i = 0, 1$. To fix this problem, we can simply set $\alpha_n = \alpha_0 + ny$ and $\beta_n = \beta_0 - nx$ to generate more identities, where $n \in \mathbb{N}$. As $n \to \infty$, the absolute values of $\alpha_n$ and $\beta_n$ approach infinity. Thus for sufficiently large $n$, the new exceptional cases do not overlap with the original ones, and the values in (3) can be represented using the new identities.

Now suppose $d$ is even. Then $d = 2q$ where $q$ is a product of primes of the form $4m + 1$. Again by Lemma 4, we can write $d = x^2 + y^2$ where $\gcd(x, y) = 1$, but this time $x \equiv y \equiv 1 \pmod 2$. We have a similar expansion as (1), and if $x\alpha + y\beta = 1$, then $\alpha \not\equiv \beta \pmod 2$ and $\alpha^2 + \beta^2 \equiv 1 \pmod 2$. Therefore we have an identity that generates all odd integers.

But in this case, shifting the solution $(\alpha, \beta)$ of (2) does not produce an identity for even integers. Therefore in (1) we consider the linear equation

$$x\alpha + y\beta = 2. \tag{4}$$

Now we pick a pair of solution $(\alpha_0, \beta_0)$, and construct the second solution pair $(\alpha_1, \beta_1)$ in a similar manner, and then

$$\begin{aligned}
\alpha_1^2 + \beta_1^2 &= (\alpha_0 + y)^2 + (\beta_0 - x)^2 \\
&= (\alpha_0^2 + \beta_0^2) + x^2 + y^2 + 2(\alpha_0 y + \beta_0 x) \\
&\equiv (\alpha_0^2 + \beta_0^2) + 2 + 2(\alpha_0 y + \beta_0 x) \pmod 4.
\end{aligned}$$

Since $x$ and $y$ are odd, and the right hand side of (4) is even, we deduce that $\alpha_0 \equiv \beta_0 \pmod 2$. Therefore $2 \mid (\alpha_0 y + \beta_0 x)$ and

$$\alpha_1^2 + \beta_1^2 \equiv \alpha_0^2 + \beta_0^2 + 2 \pmod 4.$$

Also note that $\alpha_0^2 + \beta_0^2 \equiv 0 \pmod 2$. Thus, the two identities given by

$$(xk + \alpha_i)^2 + (yk + \beta_i)^2 - (x^2 + y^2)(k)^2 = 2k + \alpha_i^2 + \beta_i^2,$$

where $i = 0, 1$, cover both integers of the form $4m$ and $4m + 2$, and hence every integer can be expressed as the form $a^2 + b^2 - dc^2$ for some integers $a, b, c$. The exceptional cases can be handled similarly as in the $d = q$ case. $\square$

# References


[1] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., 1991.

[2] A. Nowicki, The numbers $a^2 + b^2 - dc^2$, *J. Integer Seq.* **18** (2015), Article 15.2.3.

[3] S. Ramanujan, On the expression of a number in the form $ax^2 + by^2 + cz^2 + dw^2$, *Proc. Cambridge Philos. Soc.* **19** (1917), 11–21. Reprinted in *Collected Papers of Srinivasa Ramanujan*, AMS Chelsea Publishing, 2000, pp. 169–178.


---


2010 *Mathematics Subject Classification*: Primary 11D09.
*Keywords:* sum of squares, sum of two coprime squares.

---

Received July 14 2015; revised version received July 29 2015. Published in *Journal of Integer Sequences*, July 29 2015.


---


Return to Journal of Integer Sequences home page.