International Journal of Mathematics and
Computer Science, **14**(2019), no. 3, 583–590

A Characterization of Eisenstein Triples

Alessandro Cotronei

Department of Computer Science
Christian-Albrechts-Universität zu Kiel
Christian-Albrechts-Platz 4
24118 Kiel, Germany

email: aco@informatik.uni-Kiel.de

(Received March 25, 2019, Accepted April 12, 2019)

Abstract

One of the oldest problems in Mathematics it the study of Pythagorean Triples, despite a generating formula for the solutions of this equation was known since ancient times, a new solution has been found in recent times [1]. In this paper we will give a similar formula for Eisenstein Equations $x^2 + y^2 + xy = z^2$, in particular we will find a formula that explicitly generates all the triples having as first element any integer x.

1 Introduction

In this paper some classical definitions and theorems will be used, they are all in this section:

Definition 1.1 (Pythagorean Triple). *A Pythagorean Triple is a triple* (a, b, c) *of natural numbers such that* $a^2 + b^2 = c^2$.

Definition 1.2 (Eisenstein Triple). *An Eisenstein Triple is a triple* (a, b, c) *of natural numbers such that* $a^2 + b^2 + ab = c^2$, *called Eisenstein equation.*

Key words and phrases: Pythagorean and Eisenstein Triples, Diophantine.
AMS (MOS) Subject Classifications: 11D09,11D61.
ISSN 1814-0432, 2019, http://ijmcs.future-in-tech.net

The associated Diophantine equations are similar, but Pythagorean triples represent triangles with an angle of 90 degrees, Eisenstein triples represent triangles with an angle of 120 degrees.
Parametric solutions for both equations are already known:

Theorem 1.1. [2]. A triple (a, b, c) of nonnegative integer numbers is a Pythagorean triple if and only if there exist positive integers m, n, k; $m \geq n$, such that:

$$a = k\,(2mn)\,,\ b = k\left(m^2 - n^2\right),\ c = k\left(m^2 + n^2\right). \tag{1.1}$$

Theorem 1.2. [3]. A triple (a, b, c) of nonnegative integer numbers is solution of Eisenstein equation if and only if there exist positive integers m, n, k, with $m \geq n$, m and n coprime and $m \equiv n \pmod 3$, such that:

$$a = k\left(\frac{2mn + n^2}{3}\right),\ b = k\left(\frac{m^2 - n^2}{3}\right),\ c = k\left(\frac{m^2 + n^2 + mn}{3}\right). \tag{1.2}$$

One totally novel formula, completely different from (1.1), to obtain all Pythagorean triples by identifying them with a suitable class is the following:

Theorem 1.3. [1] (Amato's Formula). The integer triple (x, y, z) is a Pythagorean triple if and only if there exists $d \in C(x)$ such that:

$$x = x,\ y = \frac{x^2}{2d} - \frac{d}{2},\ z = \frac{x^2}{2d} + \frac{d}{2},$$

where

$$C(x) = \begin{cases} D(x) & \text{if x is odd.} \\ D(x) \cap P(x) & \text{if x is even.} \end{cases}$$

$D(x) = \{d \in \mathbb{N} : d \text{ divides } x^2\}$; if x is even with $x = 2^n k$ we define
$P(x) = \{d \in \mathbb{N} : d = 2^s l \text{ with } l \text{ divisor of } x^2 \text{ and } s \in \{1, 2, ..., 2n - 1\}\}$.

The main aim of this paper is to find a formula that explicitly generates all Eisenstein triples having as first element the integer x, in this way this result will be similar to Theorem 1.3, but completely different from (1.2).

2 Results

Theorem 2.1. *A natural triple (a, b, c) with $a > 0$ satisfies $a^2 + b^2 + ab = c^2$ if and only if exist unique integer*

$$d \in C_E(x) = \begin{cases} \{d \leq x : d|3x^2\} & \text{if } x \text{ is odd.} \\ \left\{d \leq x : d|3x^2, d \equiv 0 \pmod 4, \frac{3x^2}{d} \equiv 0 \pmod 4\right\} & \text{if } x \equiv 0 \pmod 4 \\ \{d \leq x : d|3x^2, d \equiv 2 \pmod 4\} & \text{if } x \equiv 2 \pmod 4 \end{cases}$$

such that

$$a = x,\ b = \frac{3x^2}{4d} - \frac{x}{2} - \frac{d}{4},\ c = \frac{3x^2}{4d} + \frac{d}{4}.$$

To prove this new formula, we need several lemmas:

Lemma 2.1. *If x is odd, then $3x^2$ can be only factored as a product of $x_1, x_2, ..., x_I$ (not necessarily primes) and the number of $x_i \equiv 3 \pmod 4$, for $1 \leq i \leq I$ is odd.*

Proof. if x is odd, then, $3x^2 \equiv 3 \pmod 4$, if we now have $3x^2 = x_1x_2...x_I$, it follows $x_1x_2...x_I \equiv 3 \pmod 4$, where each of the x_i for $1 \leq i \leq I$ is odd, then if by absurd the number of $x_i \equiv 3 \pmod 4$ is even, we have $1 \equiv 3 \pmod 4$, which is clearly impossible. □

We now start from Theorem 1.2; in particular in

$$a = k\left(\frac{2mn + n^2}{3}\right),\ b = k\left(\frac{m^2 - n^2}{3}\right),\ c = k\left(\frac{m^2 + n^2 + mn}{3}\right) \tag{2.3}$$

the following variable substitution is considered:

$$m = \frac{3x - d}{2\sqrt{kd}},\ n = \sqrt{\frac{d}{k}}. \tag{2.4}$$

With the previous definitions, the following identities hold:

$$m^2 = \frac{9x^2 - 6xd + d^2}{4kd},\ n^2 = \frac{d}{k},\ mn = \frac{3x - d}{2k}$$

if we plug the values of m^2, n^2, mn in (2.3), we obtain

$$a = x,\ b = \frac{3x^2}{4d} - \frac{x}{2} - \frac{d}{4},\ c = \frac{3x^2}{4d} + \frac{d}{4}. \tag{2.5}$$

We have to prove some properties of the last formula:

Lemma 2.2. *In the transformation* (2.4)*, if* a*,* m *and* n *are integers with* $n > 0$*, then* x *and* d *are also integers.*

Proof. First of all we notice that $\left(\frac{2mn+n^2}{3}\right)$ is a positive integer, then if we square $n = \sqrt{\frac{d}{k}}$, we have $d = n^2k$, so d is an integer, if we substitute the value of d in $m = \frac{3x-d}{2\sqrt{kd}}$, we obtain $2kmn = 3x - n^2k$ and $x = k\left(\frac{2mn+n^2}{3}\right)$, so x is an integer as well. □

Lemma 2.3. *If* $a = x,\ b = \frac{3x^2}{4d} - \frac{x}{2} - \frac{d}{4},\ c = \frac{3x^2}{4d} + \frac{d}{4}$*, then* x *and* d *are unique.*

Proof. It is clear that x is unique, if now exists r such that:

$$\frac{3x^2}{4d} + \frac{d}{4} = \frac{3x^2}{4r} + \frac{r}{4}$$

we have $d = r$, so x and d are unique. □

We want now to find out the set of d such that a, b, c are integers:

Lemma 2.4. *In* (2.5)*, if we consider* $a = x$ *as integer; then* b *and* c *are integers if and only if:*

$$d \in \begin{cases} \{d \le x : d | 3x^2\} & \text{if } x \text{ is odd.} \\ \left\{ d \le x : d | 3x^2, d \equiv 0 \pmod 4,\ \frac{3x^2}{d} \equiv 0 \pmod 4 \right\} & \text{if } x \equiv 0 \pmod 4 \\ \{d \le x : d | 3x^2,\ d \equiv 2 \pmod 4\} & \text{if } x \equiv 2 \pmod 4 \end{cases}$$

Proof. First of all we can consider $0 < d \le x$ without loss of generality; this condition is indeed equivalent to $b, c > 0$ (in particular we have $c \ge 0 \Leftrightarrow \frac{3x^2+d^2}{4d} \ge 0 \Leftrightarrow d > 0$, we can prove similarly that $b > 0 \Leftrightarrow d \le x$).
We must notice that $x \equiv d \pmod 2$ because in the opposite case $c = \frac{3x^2+d^2}{4d}$ would not be an integer.
If we now evaluate $c - b$, it is equal to $\frac{x+d}{2}$, so b is integer if and only if c is integer.
If a, b, c are integers, in particular we have $c = \frac{3x^2}{4d} + \frac{d}{4}$, so we have $3x^2 = d(4c - d)$ and $d | 3x^2$ for any x.

- Let's consider the first case (x odd), we must prove that if $d|3x^2$, then c is integer; from the first hypothesis, we have $3x^2 = dq$. We can write $d + q = 4w$ with w integer, this because d and q are indeed both odd and cannot be in the same residual class modulo 4 at the same time because of Lemma 2.1. Let's consider now the following chain of identities: $3x^2 + d^2 = dq + d^2 = d(q + d) = d(4w)$, this yields $c = \dfrac{3x^2}{4d} + \dfrac{d}{4} = w$ and c is integer (as well as a and b).

- For the second case ($x \equiv 0 \pmod 4$), we want to prove three things: First that d cannot satisfy $d \equiv 2 \pmod 4$ (we already know that it cannot be odd), second that $\dfrac{3x^2}{d} \equiv 0 \pmod 4$ and then that all d such that $d|3x^2, d \equiv 0 \pmod 4, \dfrac{3x^2}{d} \equiv 0 \pmod 4$ correspond to integer c (and b).

  - To prove the first point we consider the following identity: $3(4\bar{x})^2 + (4\bar{d} + 2)^2 = 4w(4\bar{d} + 2)$, that implies (considering the equation modulo 8) $4 \equiv 0 \pmod 8$ and we are done.
  - To prove the second point we consider $3(4\bar{x}^2) + (4\bar{d})^2 = 4w(4\bar{d})$ and $12\bar{x}^2 = \bar{d}q$ (a consequence of $d|3x^2$, $d = 4\bar{d}$ and $x = 4\bar{x}$), we obtain $q = 4(w - \bar{d})$ and $q \equiv \dfrac{3x^2}{d} \equiv 0 \pmod 4$.
  - If now $4\bar{d}q = 3(4\bar{x})^2$, we have $\bar{d}q = 12\bar{x}^2$ $3(4\bar{x})^2 + (4\bar{d})^2 = 4\bar{d}q + (4\bar{d})^2 = 4\bar{d}(q + 4\bar{d})$ and since $q \equiv \dfrac{3x^2}{d} \equiv 0 \pmod 4$, the Diophantine equation $c = \dfrac{3x^2}{4d} + \dfrac{d}{4} = w$ has always a solution for the integer $w = d + \dfrac{3x^2}{d}$.

- The final case, $x \equiv 2 \pmod 4$, is analogous to the second one, in a similar way we prove that $d \equiv 2 \pmod 4$:
  $3(4\bar{x} + 2)^2 + (4\bar{d})^2 = 4w(4\bar{d})$, that implies again the absurd $4 \equiv 0 \pmod 8$.

  We need to prove now that if $x \equiv d \equiv 2 \pmod 4$, then $q = \dfrac{3x^2}{d} \equiv 2 \pmod 4$; if $3x^2 = dq$ hold, we have $3(2)^2 \equiv 2q \pmod 4$, equivalent to $q \equiv 2 \pmod 4$ and this point is proved.
  We finally consider the chain of identities: $3x^2 + d^2 = d(q + d) = 4dw$, the last identity is verified because

$d \equiv q \equiv 2 \pmod 4$, as proved before $c = \dfrac{3x^2}{4d} + \dfrac{d}{4}$ is equivalent to the integer w.

□

We can now prove the main result:

Proof. $\Longrightarrow$
If (a, b, c), $a > 0$ are integers satisfying $a^2 + b^2 + ab = c^2$, then exist for Theorem 1.2, integer m, n; satisfying in particular $m \geq n$, $n > 0$ such that

$$a = k\left(\frac{2mn + n^2}{3}\right),\ b = k\left(\frac{m^2 - n^2}{3}\right),\ c = k\left(\frac{m^2 + n^2 + mn}{3}\right).$$

Applying now substitution (2.4), we obtain:

$$a = x, b = \frac{3x^2}{4d} - \frac{x}{2} - \frac{d}{4},\ c = \frac{3x^2}{4d} + \frac{d}{4}.$$

In particular these x and d are always integers for Lemma 2.2 and unique for Lemma 2.3, finally $d \in C_E(x)$, because in the opposite case, for Lemma 2.4, then b and c would not be integers.
The implication $\Longleftarrow$ is easily verified, since the identity

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

is valid $\forall x, d > 0$, so in particular for x integer and $d \in C_E(x)$.

Remark 2.1. *If $d = x$, then the trivial solution $(x, 0, x)$ of Eisenstein equation is generated.*

The previous theorem has this interesting corollary:

Corollary 2.1. *An odd number $p \neq 9$ is prime if and only if if the only solutions for Eisenstein equation $p^2 + b^2 + pb = c^2$ are given by*
$C_E(p) = \{1, 3, p\}$.

Proof. If $p = 3$, then the Corollary is verified with the degenerated set
$C_E(3) = \{1, 3\}$.
$\Longrightarrow$
If p is an odd prime, $p \neq 3$, then $C_E(p) = \{d \leq p : d | 3p^2\} = \{1, 3, p\}$.
$\Longleftarrow$
If $p \notin \{3, 9\}$ and $C_E(p) = \{1, 3, p\}$, then p is odd, if by absurd $p = st$, where

t is not 3 without loss of generality; we have $C_E(p) = \{d \leq st : d|3(st)^2\}$ and the last set always contains the subset $\{1, 3, t, st\}$; we have obtained a contradiction. □

Remark 2.2. *Theorem* 1.3 *can be proved in an analogous way, by using the substitution*

$$m = \frac{x}{\sqrt{2kd}},\ n = \sqrt{\frac{d}{2k}}$$

in Theorem 1.1 *and steps similar with Theorem* 2.1 *and related lemmas.*

Example 2.1. *We give a table of the solutions of Eisenstein equation for* $1 \leq x \leq 24$*:*

$x = 1;\ d = 1\ (1, 0, 1).$
$x = 2;\ d = 2\ (2, 0, 2).$
$x = 3;\ d = 1\ (3, 5, 7),\ d = 3\ (3, 0, 3).$
$x = 4;\ d = 4\ (4, 0, 4).$
$x = 5;\ d = 1\ (5, 16, 19),\ d = 3\ (5, 3, 7),\ d = 5\ (5, 0, 5).$
$x = 6;\ d = 2\ (6, 10, 14),\ d = 6\ (6, 0, 6).$
$x = 7;\ d = 1\ (7, 33, 37),\ d = 3\ (7, 8, 13),\ d = 5\ (7, 0, 7).$
$x = 8;\ d = 4\ (8, 7, 13),\ d = 8\ (8, 0, 8).$
$x = 9;\ d = 1\ (9, 56, 61),\ d = 3\ (9, 15, 21),\ d = 9\ (9, 0, 9).$
$x = 10;\ d = 2\ (10, 32, 38),\ d = 6\ (10, 6, 14),\ d = 10\ (10, 0, 10).$
$x = 11;\ d = 1\ (11, 85, 91),\ d = 3\ (11, 24, 31),\ d = 11\ (11, 0, 11).$
$x = 12;\ d = 4\ (12, 20, 28),\ d = 12\ (12, 0, 12).$
$x = 13;\ d = 1\ (13, 120, 127),\ d = 3\ (13, 35, 43),\ d = 13\ (13, 0, 13).$
$x = 14;\ d = 2\ (14, 66, 74),\ d = 6\ (14, 16, 26),\ d = 14\ (14, 0, 14).$
$x = 15;\ d = 1\ (15, 161, 169),\ d = 3\ (15, 48, 57),\ d = 5\ (15, 25, 35),\ d = 9\ (15, 9, 21),\ d = 15\ (15, 0, 15).$
$x = 16;\ d = 4\ (16, 39, 49),\ d = 8\ (16, 14, 26),\ d = 12\ (16, 5, 19),\ d = 16\ (16, 0, 16).$
$x = 17;\ d = 1\ (17, 208, 217),\ d = 3\ (17, 63, 73),\ d = 17\ (17, 0, 17).$
$x = 18;\ d = 2\ (18, 112, 122),\ d = 6\ (18, 30, 42),\ d = 18\ (18, 0, 18).$
$x = 19;\ d = 1\ (19, 261, 271),\ d = 3\ (19, 80, 91),\ d = 19\ (19, 0, 19).$
$x = 20;\ d = 4\ (20, 64, 76),\ d = 12\ (20, 12, 28),\ d = 20\ (20, 0, 20).$
$x = 21;\ d = 1\ (21, 320, 331),\ d = 3\ (21, 99, 111),\ d = 7\ (21, 35, 49),\ d = 9\ (21, 24, 39),\ d = 21\ (21, 0, 21).$
$x = 22;\ d = 2\ (22, 170, 182),\ d = 6\ (22, 48, 62),\ d = 22\ (22, 0, 22).$
$x = 23;\ d = 1\ (23, 285, 397),\ d = 3\ (23, 120, 133),\ d = 23\ (23, 0, 23).$
$x = 24;\ d = 4\ (24, 95, 109),\ d = 8\ (24, 40, 56),\ d = 12\ (24, 21, 39),\ d = 16\ (24, 11, 31),\ d = 24\ (24, 0, 24).$

Acknowledgements. The author of this paper wishes to thank Roberto Amato for his valuable suggestions that led to an improvement of this work and the anonymous referee for the interesting ideas on future development of this topic.

References

[1] R. Amato, *A characterization of pythagorean triples*, JP Journal of Algebra, Number Theory and Applications, **39,** no. 2, 2017, 221.

[2] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser, 2010.

[3] F. Barnes, *Pythagorean Triples, etc.*, http://www.geocities.ws/fredlb37/node9.html.

[4] W. Sierpiñski, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, 1988.