INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A19

A CHARACTERIZATION OF ALL EQUILATERAL TRIANGLES IN $\mathbb{Z}^3$

Ray Chandler
Associate Editor of OEIS
RayChandler@alumni.tcu.edu

Eugen J. Ionascu[1]
Department of Mathematics, Columbus State University, Columbus, GA 31907, US
ionascu_eugen@colstate.edu

Received: 1/5/08, Accepted: 4/19/08, Published: 5/8/08

Abstract

This paper is a continuation of the work started by the second author in a series of papers. We extend to the general case the characterization previously found for those equilateral triangles in $\mathbb{R}^3$ whose vertices have integer coordinates. In this earlier work, we made use of the hypothesis that (a, b, c) is a non-degenerate primitive solution of $a^2+b^2+c^2 = 3d^2$. This condition is now eliminated. Although degenerate solutions present less interest as a result, we state a conjecture which gives a characterization for the existence of such solutions. An approximate extrapolation formula for the sequence $ET(n)$ of all equilateral triangles with vertices in $\{0, 1, 2, ..., n\}^3$ is given and the asymptotic behavior of this sequence is analyzed.

1. Introduction

It turns out that equilateral triangles in $\mathbb{Z}^3$ exist and there are unexpectedly many. Just to give an example, if we restrict our attention only to the cube $\{0, 1, 2, ..., 2007\}^3$ we have 52,783,138,012,302,384 of them. In [1] it was shown the first part of the following theorem and the second part about the converse was only proven under the hypothesis that $gcd(d, a) = 1$ or $gcd(d, b) = 1$ or $gcd(d, c) = 1$. The main result of this paper is to show that one can drop this condition.

[1] Honorary Member of the Romanian Institute of Mathematics "Simion Stoilow"

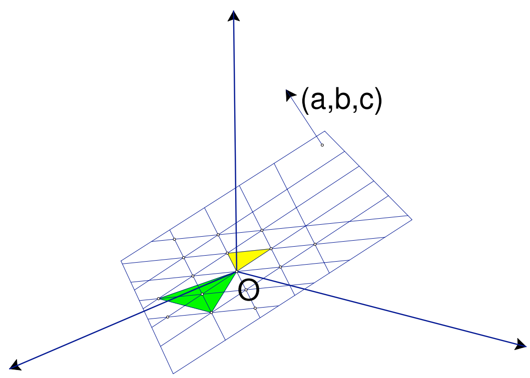

Figure 1: Plane $\mathcal{P}_{a,b,c}$ and a few triangles given by parametrization (1) and (2)

Theorem 1. *Let a, b, c, d be odd positive integers such that $a^2 + b^2 + c^2 = 3d^2$ and $gcd(a, b, c) = 1$. Then the points $P(u, v, w)$ and $Q(x, y, z)$ whose coordinates given by*

$$\begin{cases} u = m_u m - n_u n, \\ v = m_v m - n_v n, \\ w = m_w m - n_w n, \end{cases} \quad \textit{and} \quad \begin{cases} x = m_x m - n_x n, \\ y = m_y m - n_y n, \\ z = m_z m - n_z n, \end{cases} \quad m, n \in \mathbb{Z}, \tag{1}$$

with

$$\begin{cases} m_x = -\frac{1}{2}[db(3r+s) + ac(r-s)]/q, & n_x = -(rac + dbs)/q \\ m_y = \frac{1}{2}[da(3r+s) - bc(r-s)]/q, & n_y = (das - bcr)/q \\ m_z = (r-s)/2, & n_z = r \end{cases}$$
$$\textit{and} \tag{2}$$
$$\begin{cases} m_u = -(rac + dbs)/q, & n_u = -\frac{1}{2}[db(s-3r) + ac(r+s)]/q \\ m_v = (das - rbc)/q, & n_v = \frac{1}{2}[da(s-3r) - bc(r+s)]/q \\ m_w = r, & n_w = (r+s)/2 \end{cases}$$

where $q = a^2 + b^2$ and (r, s) is a suitable solution of $2q = s^2 + 3r^2$ which makes all the numbers in (2) integers, together with the origin (O(0,0,0)) forms an equilateral triangle in $\mathbb{Z}^3$ contained in the plane $\mathcal{P}_{a,b,c} := \{(\alpha, \beta, \gamma) | a\alpha + b\beta + c\gamma = 0\}$ and having sides-lengths equal to $d\sqrt{2(m^2 - mn + n^2)}$.

Conversely, there exists a choice of the integers r and s such that given an arbitrary equilateral triangle in $\mathbb{R}^3$ with one of its vertices the origin, and the other two having integer coordinates contained in the plane $\mathcal{P}_{a,b,c}$, then these two vertices must be of the form (1) and (2) for some integer values m and n.

The conditions

$$gcd(a, b, c) = 1, \; min(gcd(d, a), gcd(d, b), gcd(d, c)) > 1 \tag{3}$$

define (a, b, c) as a *degenerate solution* of the Diophantine equation

$$a^2 + b^2 + c^2 = 3d^2. \tag{4}$$

Equation (4) has, for every odd number d, at least one nontrivial decomposition (i.e., those for which $gcd(a, b, c) = 1$). However, the first d that admits degenerate decompositions is 1105 which by coincidence is the second Carmichael number. There are exactly seven degenerate decompositions of $d = 1105$:

$$(a, b, c) \in \{(731, 1183, 1315), (475, 1309, 1313), (299, 493, 1825),\\ (1027, 1139, 1145), (187, 415, 1859), (265, 533, 1819), (493, 1001, 1555)\}.$$

The connection with Carmichael numbers goes a little further. Carmichael numbers have at least three prime factors and numerical evidence suggests that the following conjecture is true:

Conjecture: *The Diophantine equation (4) has degenerate solutions if and only if d has at least three distinct prime factors of the form $4k + 1$, $k \in \mathbb{N}$.*

One can easily prove the necessity part of this conjecture. Fortunately, we did not have to go into details of the study of degenerate solutions of (4) because, as we mentioned, this condition was not necessary for our result to hold true in general.

Our study started with the intent of computing the sequence $ET(n)$ of all equilateral triangles with vertices in $\{0, 1, 2, ..., n\}$. These values were calculated by the first author for $n \leq 3315$ using an improved version of the code published in [2] and translated into Mathematica (see A102698 in The On-Line Encyclopedia of Integer Sequences, [4]).

One of the parametrizations like in (1) and (2), in the case $a = 731$, $b = 1183$ and $c = 1315$, is shown below:

$$P = (901m - 1428n, -1157m + 221n, 540m + 595n),\\ Q = (-527m - 901n, -936m + 1157n, 1135m - 540n), \qquad m, n \in \mathbb{Z}.$$

Observe that for this example, $gcd(a, d) = 17$, $gcd(b, d) = 13$, and $gcd(c, d) = 5$. There is something special about these numbers and the above parametrization: the first coordinates of P and Q are multiples of 17, the second coordinates are divisible by 13 and the last components are multiples of 5. This is a fact that we will show in general.

Although for various solutions of r and s we may get formally different parametrizations, they are all equivalent in the sense that one can be obtained from another by changing the variables in the expected ways:

$$(m, n) \to (-m, -n),\ (m, n) \to (m - n, m),\ (m, n) \to (n - m, n),\\ (m, n) \to (m - n, -n),\ \textit{and}\ (m, n) \to (n - m, -m). \tag{5}$$

These changes of variables leave invariant the quadratic form involved in the side-length formula of these triangles given in Theorem 1. The various points given by (1) and (2) define a lattice of points or the vertices of a regular tessellation of the plane $\mathcal{P}_{a,b,c}$ with triangles as illustrated in Figure 1.

2. Proof of Theorem 1

The first part of the Theorem 1 follows from [1]. For the second part we are going to reconstitute some of the details started in the proof of the particular case: $gcd(d, c) = 1$.

Let us start with a triangle in $\mathcal{P}_{a,b,c}$ say $\triangle OP'Q'$ with $P'(u_0, v_0, w_0)$ and $Q'(x_0, y_0, z_0)$ having integer coordinates. By Theorem 4 in [1] we have

$$\begin{cases} x_0 = \dfrac{u_0}{2} \pm \dfrac{cv_0 - bw_0}{2d} \\ y_0 = \dfrac{v_0}{2} \pm \dfrac{aw_0 - cu_0}{2d} \\ z_0 = \dfrac{w_0}{2} \pm \dfrac{bu_0 - av_0}{2d}, \end{cases} \tag{6}$$

for some choice of the signs. This means that d must divide $cv_0 - bw_0$, $aw_0 - cu_0$ and $bu_0 - aw_0$. So, we need to look at the following system of linear equations in m and n:

$$\begin{cases} m_u m - n_u n = u_0, \\ m_v m - n_v n = v_0, \\ m_w m - n_w n = w_0. \end{cases} \tag{7}$$

By the Kronecker-Capelli theorem this linear system of equations has a solution if and only the rank of the main matrix is the same as the rank of the extended matrix. Since $m_v n_w - m_w n_v = ad$, $m_w n_u - m_u n_w = bd$ and $m_u n_v - m_v n_u = cd$ (one can check these calculations based on the definitions in (2)) then the rank of the main matrix is two and the rank of the extended matrix is also two because its determinant is $u_0 ad + v_0 bd + w_0 dc = 0$. This implies that (7) has a unique real (in fact rational) solution in m and n.

We want to show that this solution is in fact an integer solution. Solving for n from each pair of equations in (7) we get

$$n = \frac{v_0 m_w - w_0 m_v}{ad} = \frac{w_0 m_u - u_0 m_w}{bd} = \frac{u_0 m_v - v_0 m_u}{cd}. \tag{8}$$

Because $gcd(a, b, c) = 1$, there exist integers a', b', c' such that $aa' + bb' + cc' = 1$. Then one can see that

$$n = \frac{a'(v_0 m_w - w_0 m_v) + b'(w_0 m_u - u_0 m_w) + c'(u_0 m_v - v_0 m_u)}{d} \tag{9}$$

Next, from (9) we observe that in order for n to be an integer it is enough to prove that d divides $v_0 m_w - w_0 m_v$, $w_0 m_u - u_0 m_w$ and $u_0 m_v - v_0 m_u$. Hence we calculate for example $v_0m_w - w_0m_v$ in more detail:

$$v_0m_w - w_0m_v = v_0r - \frac{das - rbc}{q}w_0 = \frac{v_0qr - (das - rbc)w_0}{q} =$$

$$\frac{-dasw_0 + v_0(3d^2 - c^2)r + rbcw_0}{q} = \frac{c(bw_0 - v_0c)r + 3rv_0d^2 - dasw_0}{q}.$$

From (6) we see that $bw_0 - v_0c = \pm d(2x_0 - u_0)$. Hence,

$$v_0m_w - w_0m_v = \frac{d[\pm c(2x_0 - u_0)r + 3rv_0d - asw_0]}{q}. \tag{10}$$

Assuming that $gcd(d, c) = \zeta$ we can write $d = \zeta d_1$ and $c = \zeta c_1$ with $gcd(d_1, c_1) = 1$. Also we see that ζ^2 must divide $q = 3d^2 - c^2$ so let us write $q = \zeta^2 q_1$. If p is a prime dividing ζ, it must be an odd prime and if it is of the form $4k + 3$ it must divide a and b which is contradicting the assumption that $gcd(a, b, c) = 1$. Therefore it must be a prime of the form $4k + 1$. Hence q_1 is still a sum of two squares.

In the proof of Theorem 13 in [1] one can choose r and s with the extra condition that r and s are divisible by ζ. Indeed, Lemma 14 in [1] is applied to $(ac)^2 + 3(db)^2 = \zeta^2[(ac_1)^2 + 3(d_1b)^2]$ and to $q = \zeta^2 q_1$ but instead one can apply it to $(ac_1)^2 + 3(d_1b)^2$ and to q_1 giving, let us, say r_1 and s_1. Then we put $r = \zeta r_1$ and $s = \zeta s_1$ and then all the arguments there go as stated. Then from (10) we see that

$$\begin{aligned} v_0m_w - w_0m_v &= \frac{d[\pm c(2x_0 - u_0)r + 3rv_0d - asw_0]}{q} \\ &= \frac{\zeta d_1[\pm\zeta c_1(2x_0 - u_0)\zeta r_1 + 3\zeta r_1v_0\zeta d_1 - a\zeta s_1w_0]}{\zeta^2 q_1} \\ &= \frac{\zeta^2 d_1[\pm c_1(2x_0 - u_0)r_1\zeta + 3r_1v_0d_1\zeta - as_1w_0]}{\zeta^2 q_1} = \frac{d_1\xi}{q_1}, \end{aligned} \tag{11}$$

where $\xi = \pm c_1(2x_0 - u_0)r_1\zeta + 3r_1v_0d_1\zeta - as_1w_0$. This implies that d_1 must divide $v_0m_w - w_0m_v$ since $gcd(d_1, q_1) = 1$. In a similar way we can show that d_1 divides $w_0m_u - u_0m_w$ and $u_0m_v - v_0m_u$. Hence, from (9) we see that n is a rational with denominator ζ. Similar arguments will give us that m is of the same form.

The triangle having the coordinates as in (1) and (2) with these m and n (even if they are rational) will have same formula for the side-lengths:

$$l^2 = 2d^2(m^2 - mn + n^2).$$

This whole construction can be repeated for a or b instead of c and we obtain that

$$l^2 = 2d^2(m_1^2 - m_1n_1 + n_1^2),$$

for some rational numbers m_1, n_1 with denominator $\eta = gcd(d, b)$. Since $gcd(\zeta, \eta) = 1$ we see that $m^2 - mn + n^2 = m_1^2 - m_1n_1 + n_1^2$ must be an integer. Therefore,

$$l^2 = 2d^2(\alpha^2 - \alpha\beta + \beta^2),\ for\ some\ \alpha, \beta \in \mathbb{Z}. \tag{12}$$

On the other hand if $u_0^2 + v_0^2 + w_0^2 = l^2$ and ζ divides d we can see that

$$u_0^2 + v_0^2 + w_0^2 \equiv 0\ (mod\ \zeta^2). \tag{13}$$

We also know that $au_0 + bv_0 + cw_0 = 0$ and hence $a^2u_0^2 = b^2v_0^2 + 2bcv_0w_0 + c^2w_0^2$. This implies $a^2u_0^2 \equiv b^2v_0^2 + 2bcv_0w_0 \pmod{\zeta^2}$. But $a^2 + b^2 = 3d^2 - c^2 \equiv 0 \pmod{\zeta^2}$ too and then $a^2(u_0^2 + v_0^2) \equiv 2bcv_0w_0 \pmod{\zeta^2}$ which combined with (13) gives

$$a^2w_0^2 + 2bcv_0w_0 \equiv 0\ (mod\ \zeta^2). \tag{14}$$

Because we must have $gcd(a, \zeta) = 1$, (14) implies that ζ divides w_0. Indeed, if p is a prime that has exponent one in the decomposition of ζ then (14) gives in particular $w_0^2 \equiv 0 \pmod{p}$ and so p must divide w_0. If the exponent of p in ζ is two, then (14) in particular implies that w_0 is divisible by p but then $aw_0^2 \equiv 0 \pmod{p^3}$ which implies p^2 divides w_0. Inductively if the exponent of p in ζ is k then this must be true for w_0 too. Hence we must have ζ a divisor of w_0 so $w_0 = \zeta w_0'$.

Now we can go back to (11) and observe that we can rewrite it as

$$v_0r - w_0m_v = \frac{\zeta d_1\xi'}{q_1}, \tag{15}$$

where $\xi' = \pm c_1(2x_0 - u_0)r_1 + 3r_1v_0d_1 - as_1w_0'$. Now we observe that the left hand side of (15) is a multiple of ζ since r and w_0 are. After simplification with ζ this will show that q_1 must divide in fact ξ' and so d divides $v_0m_w - w_0m_v$. Similar arguments can be used to show that d divides $w_0m_u - u_0m_w$. Finally, for the term $u_0m_v - v_0m_u$ that appears in (9), we obtain a similar expression

$$u_0m_v - v_0m_u = \frac{\zeta d_1[-c_1w_0s_1 \mp 2r_1c_1(2z_0 - w_0)]}{q_1} = \frac{\zeta d_1\xi''}{q_1}, \tag{16}$$

which shows as before that d_1 divides $u_0m_v - v_0m_u$. On the other hand since $au_0 + bv_0 + cw_0 = 0$ and $am_u + bm_v + cm_w = 0$, we obtain that $a(u_0m_v - v_0m_u) = \zeta c_1(rv_0 - w_0m_v)$. This last relation, together with the fact that $gcd(\zeta, a) = 1$ gives that ζ must divide $u_0m_v - v_0m_u$. Again, (16) can be simplified by ζ and that implies that q_1 must divide ξ''. Therefore d divides $u_0m_v - v_0m_u$ too.

Using (9), n must be an integer and so should be m. Changing the variables as in (5), one of the corresponding triangles given by (1) is going to match with the triangle $OP'Q'$.

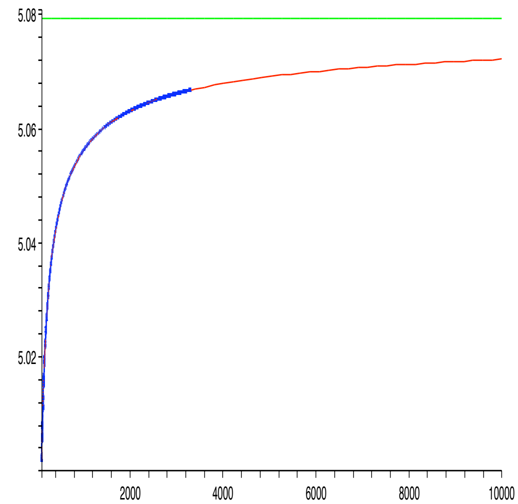

Figure 2: The graph of g extrapolating f over the interval $[100, 10000]$

Remark: One can see that the condition on r and s to be divisible by ζ is implied by asking only that the numbers in (2) be integers. Indeed, given a choice of r and s as required in Theorem 1, they will define by (1), in which $m = 1$ and $n = 0$, an equilateral triangle with integer coordinates. According to the above proof of Theorem 1, $w = r$ and $z = (r-s)/2$ must be divisible by ζ. This implies that r and s must be multiples of ζ. As a corollary any parametrization as in the Theorem 1 is unique up to the transformations (5).

3. Behavior of the Sequence $ET(n)$

The calculations of the $ET(n)$ for all $n \leq 3315 = (3)(5)(13)(17)$ gave us enough data to be able to extrapolate the graph of $n \xrightarrow{f} \frac{\ln(ET(n))}{\ln(n+1)}$ as shown in Figure 2. The function we used to extrapolate is of the form $g(x) = a + \frac{b}{\sqrt{x}+c}$ having clearly a as limit at infinity. Then we made it agree with f on three points. That gave us $a := 5.079282921$, $b := -0.7091588389$, and $c := -0.8403164433$. Numerically then we discovered that the average of $|f(k) - g(k)|$ over all values of $k = 100, ..., 3315$ is approximately 0.000250721.

One conjecture that we would like to make here is that $f(n)$ is a strictly increasing sequence and then as result it is convergent to a constant $C \approx 5.08$.

The graph of the "derivative" of $ET(n)$ (Figure 3) is almost like the graph of $h(x) = C(x+1)^k$ where $k := 4.151431798$ and $C := 2.660972140$. The third difference of $ET(n)$ as represented in Figure 4 seems to bring a chaotic flavor to this sequence and it is saying in a certain sense that no simple formula for $ET(n)$ can exist.

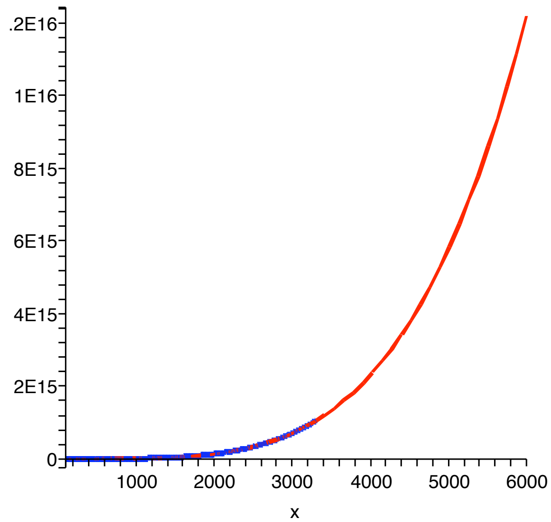

Figure 3: The graph of $n \to ET(n+1) - ET(n)$, $n = 100 \ldots 6000$

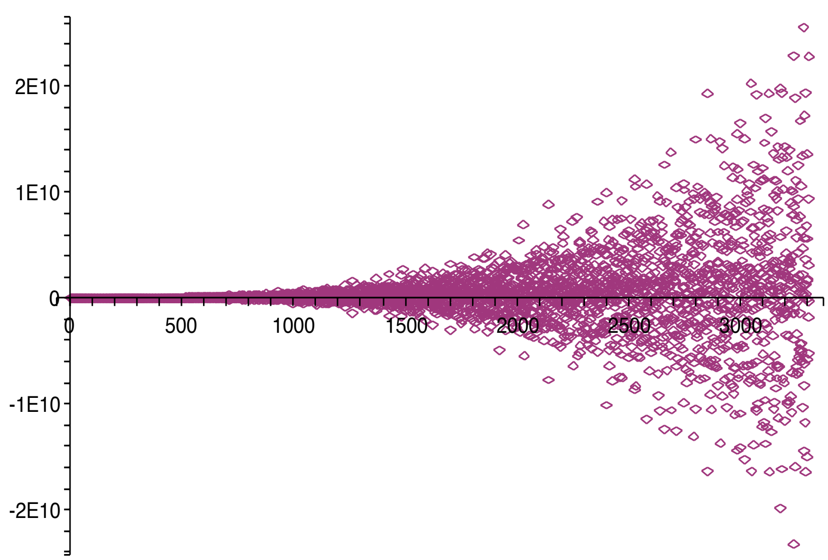

Figure 4: $\Delta^3 ET(n)$

References

[1] E. J. Ionascu, *A parametrization of equilateral triangles having integer coordinates*, J. Integer Seqs., Vol. 10 (2007), # 07.6.7

[2] E. J. Ionascu, *Counting all equilateral triangles in* $\{0, 1, ..., n\}^3$, Acta Math. Univ. Comenianae, vol. LXXVII, **1**(2008), pp.129-140.

[3] C. J. Moreno and S.S. Wagstaff, JR. *Sums of Squares*, Chapman & Hall/CRC, 2006.

[4] Neil J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, 2005, published electronically at `http://www.research.att.com/~njas/sequences/`.