NNTDM 3 (1997) 1, 41-51

The Anatomy of Odd-Exponent Diophantine Triples

J. V. Leyendekkers and J. M. Rybak
The University of Sydney, 2006, Australia

A. G. Shannon
The University of Technology, Sydney, 2007, Australia

Abstract

In similar manner to the analysis for even-exponent triples, this paper uses the equivalence classes of the modular ring $\mathbb{Z}_6$ to show why the diophantine equation $d^m = e^m + f^m$, where m is odd, is limited to $m = 1$ in $\mathbb{Z}_6$.

1. Introduction

We have previously analysed the diophantine equation [1]

$$c^{2n} = b^{2n} + a^{2n} \tag{1.1}$$

using an approach centred on the equivalence classes of the modular ring $\mathbb{Z}_6$ [2]. In this paper we also analyse for odd m the Diophantine equation in $\mathbb{Z}_6$

$$c^m = b^m + a^m \tag{1.2}$$

This is a more complex situation in the context of $\mathbb{Z}_6$ as a much larger number of classes have to be considered. We first consider the cubic form and then generalise to cover all odd m.

In a sense, of course, if $z = a + b$

$$x^p + y^p \equiv z^p \qquad (\mathrm{mod}\, p)$$

but we are concerned with structure of the diophantine equations, not in the context of Kummer's ideals, but in the context of equivalence classes of $\mathbb{Z}_6$.

2. Cubic Triples

There are thirteen possible combinations of the classes for odd-exponent triples. This number is arrived at by taking all possible combination of classes for $< c, b, a >$ and eliminating those that do not conform to the $\mathbb{Z}_6$ rules of addition [2] giving equation (1.2), or are not primitive. The odd powers of c, b and a fall in the same class as c, b and a, respectively, since for $x \in \mathbb{Z}_6, x^m = x$. Unlike even powered triples, c can be even with a and b both odd in the present case. Five class-sets of this type occur here.

The function for a number in class $\bar{i}$ in $\mathbb{Z}_6$ is given by $(6r_i + (i-3))$ where r_i is the row in class $\bar{i}$. Thus, if this number is cubed, the function becomes:

$$(6r_i + (i-3))^3 = Ar^3 + Br^2 + Cr + D \tag{2.1}$$

where $A = 6^3$, $B = 3(i-3) \times 6^2$, $C = 3(i-3)^2 \times 6$ and $D = (i-3)^3$. Table 1 lists A, B, C and D for the six classes.

Classes	r function	A	B	C	D
$\bar{1}$	$6r_1 - 2$	6^3	-18×12	3×24	-8
$\bar{2}$	$6r_2 - 1$	6^3	-9×12	18	-1
$\bar{3}$	$6r_3$	6^3	–	–	–
$\bar{4}$	$6r_4 + 1$	6^3	9×12	18	1
$\bar{5}$	$6r_5 + 2$	6^3	18×12	3×24	8
$\bar{6}$	$6r_6 + 3$	6^3	9×36	18×9	27

Table 1: Coefficients for cube of function r

Of course, the cube could be represented simply by $(6R_i + (i-3))$ where R_i is the row containing the cube. However, this form is of no direct use here since it would obscure the cubic characteristic of the number.

For each class set, we take c in class $\bar{i}$, b in class $\bar{j}$ and a in class $\bar{k}$.

$$c^3 - b^3 - a^3 = 6^3 f(r^3) + f(r^2) + f(r) + E \tag{2.2}$$

where $f(r^3) = (r_i^3 - r_j^3 - r_k^3)$, $f(r^2) = B_i r_i^2 - B_j r_j^2 - B_k r_k^2$, $f(r) = C_i r_i - C_j r_j - C_k r_k$ and $E = D_i - D_j - D_k$.

For example, for the $< \overline{2}, \overline{1}, \overline{4} >$ triple

$$6^3(r_2^3 - r_1^3 - r_4^3) - 3 \times 36(r_2^2 - 2r_1^2 + r_4^2) + 18(r_2 - 4r_1 - r_4) + 6 = 0 \quad (2.3)$$

Dividing throughout by 18 gives the coefficients $\overline{A} = 12$ for $f(r^3)$, $\overline{B} = -6$ for $f(r^2)$, $\overline{C} = 1$ for $f(r)$ and $\overline{E} = (1/3)$. A bar over the coefficient symbols indicates division by a suitable factor. Thus, no integer solution exists for this set. Another three class sets give the same result (Table 2).

No	Classes	$\overline{A}$	$\overline{B}$	$\overline{C}$	$\overline{E}$
1	$< \overline{2}, \overline{1}, \overline{4} >$	12	-6	1	$1/3$
2	$< \overline{4}, \overline{5}, \overline{2} >$	12	6	1	$-1/3$
3	$< \overline{1}, \overline{2}, \overline{2} >$	12	-6	1	$-1/3$
4	$< \overline{5}, \overline{4}, \overline{4} >$	12	6	1	$1/3$

Table 2: Coefficients for $f(r^j), j = 1, 2, 3$

The remaining nine class-sets are treated as follows. We divide equation (2.2) by w, the lowest factor to give an apparent non-integer residual. This residual involves the r values and has the form $((r_i + r_k) + d)/w$ or $((r_j + r_k) + d)/w$, with $d = -1, 0$ or 1. For example, for the $< \overline{2}, \overline{3}, \overline{2} >$ set the residual is $(r_2 - r_2')/6$. Since, for this set, $r_2 = (c + 1)/6$ and $r_2' = (a + 1)/6$, we get:

$$c = a + 36t \quad (2.4)$$

where t is the value of the residual. The aim is to show that t cannot be an integer.

Equation (2.4) is now cubed so that a cubic in t is formed and this cubic is then solved. The Appendix illustrates this for primitive Pythagorean triples..

No	Classes	$f(r^3)$	$f(r^2)$	$f(r)$	Residual
5	$<\overline{6},\overline{5},\overline{4}>$	$6(r_6^3-r_5^3-r_4^3)$	$3(3r_6^2-2r_5^2-r_4^2)$	$2(2r_6-r_5)$	$(r_6-r_4+1)/2$ $c=a-4(1-3t)$
6	$<\overline{5},\overline{2},\overline{6}>$	$6(r_5^3-r_2^3-r_6^3)$	$3(2r_5^2+r_2^2-3r_6^2)$	$2(r_5-2r_6)$	$-(r_2+r_6+1)/2$ $b=-(a+4(1-3t))$
7	$<\overline{2},\overline{3},\overline{2}>$	$2(r_2^3-r'^3_2-r_3^3)$	$-(r_2^2-r'^2_2)$	–	$(r_2-r'_2)/6$ $c=a+36t$
8	$<\overline{4},\overline{3},\overline{4}>$	$2(r_4^3-r'^3_4-r_3^3)$	$(r_4^2-r'^2_4)$	–	$(r_4-r'_4)/6$ $c=a+36t$
9	$<\overline{6},\overline{1},\overline{2}>$	$6(r_6^3-r_1^3-r_2^3)$	$3(3r_6^2+2r_1^2+r_2^2)$	$(2(2r_6-r_1)+1)$	$(r_6-r_2)/2$ $c=a+4(1+3t)$
10	$<\overline{4},\overline{1},\overline{6}>$	$6(r_4^3-r_1^3-r_6^3)$	$3(r_4^2+2r_1^2-3r_6^2)$	$-2(r_1+2r_6)$	$(r_4-r_6-1)/2$ $c=a+4(1+3t)$
11	$<\overline{1},\overline{4},\overline{6}>$	$6(r_1^3-r_4^3-r_6^3)$	$-3(2r_1^2+r_4^2+3r_6^2)$	$(2(r_1-2r_6)-1)$	$-(r_4+r_6)/2$ $b=-a+4(1+3t)$
12	$<\overline{3},\overline{2},\overline{4}>$	$2(r_3^3-r_2^3-r_4^3)$	$(r_2^2-r_4^2)$	–	$-(r_2+r_4)/6$ $a=-b+36t$
13	$<\overline{2},\overline{5},\overline{6}>$	$6(r_2^3-r_5^3-r_6^3)$	$-3(r_2^2+2r_5^2+3r_6^2)$	$(-2(r_5+2r_6)-1)$	$(r_2-r_6)/2$ $c=a-4(1-3t)$

Table 3: Residual functions

As can be seen from Table 3 the residual functions in t are of two types:

$$x = \pm y \pm 4(1 \pm 3t) \tag{2.5}$$

$$x = \pm y + 36t \tag{2.6}$$

However, in each case the roots for t are found to be equal and non-integer. An example for each of the equations (2.5) and (2.6) should therefore suffice for the nine sets.

Set $<\overline{6},\overline{5},\overline{4}>$

Here

$$c = 6r_6 + 3 \tag{2.7}$$

$$b = 6r_5 + 2 \tag{2.8}$$

$$a = 6r_4 + 1 \tag{2.9}$$

The residual is $(r_6 - r_4 + 1)/2$ (Table 3) and since $r_6 = (c-3)/6$ and $r_4 = (a-1)/6$, we get $(c - a + 4)/12$ for the residual. Let this quantity equal t, so that:

$$c = a - 4(1 - 3t) \tag{2.10}$$

Cubing both sides of equation (2.10) yields:
$(c^3 - a^3) = f(a,t) = b^3$, so that $t^3 + ((a-4)/4)t^2 + (1/3)((a-4)/4)^2 t$

$$- a((a-4)/4)/36 - 1/27 - b^3/64 \times 27 = 0 \tag{2.11}$$

With A, B, C as the roots,

$$-((a-4)/4) = A + B + C \tag{2.12}$$

$$(1/3)((a-4)/4)^2 = AB + AC + BC \tag{2.13}$$

Thus $(A + B + C)^2$ equals $3(AB + AC + BC)$ so that

$$A^2 + B^2 + C^2 = AB + AC + BC \tag{2.14}$$

Hence $A = B = C$ and

$$A = -((a-4)/12) \tag{2.15}$$

But a is odd so that the numerator is odd and A cannot be an integer. (See the Appendix.)

Set $< \overline{4}, \overline{3}, \overline{4} >$

Here

$$c = 6r_4 + 1 \tag{2.16}$$

$$b = 6r_3 \tag{2.17}$$

$$a = 6r_4' + 1 \tag{2.18}$$

The residual is $(r_4 - r_4')/6$ so that,

$$c = a + 36t \tag{2.19}$$

When cubed, this gives:

$$t^3 + (a/12)t^2 + (1/3)(a/12)^2 t - b^3/(36)^3 = 0 \tag{2.20}$$

Thus

$$-(a/12) = A + B + C \tag{2.21}$$

$$(1/3)(a/12)^2 = AB + AC + CB \tag{2.22}$$

Hence

$$A^2 + B^2 + C^2 = AB + AC + CB \tag{2.23}$$

so that $A = B = C$ and

$$A = -(a/36) \tag{2.24}$$

But a is odd and prime to 3 so that no integer solution is possible.

Since $ABC = A^3$, for the class $< \overline{6}, \overline{5}, \overline{4} >$ we obtain from equations (2.15) and the non-t term of equation (2.11) that $(a^3 = -b^3)$, so that $c = 0$. Whereas, for the class $< \overline{4}, \overline{3}, \overline{4} >$ from equation (2.24) and the non-t term of equation (2.20) we find $(a^3 = b^3)$ so that $c = (2^{(1/3)})a$.

This yields the two forms, namely equations (2.5) and (2.6).

3. General Solution for Odd Exponent Triples

In the general case for $n > 3$, the residual is of the form

$$(6^n(r_i^n - r_j^n - r_k^n) + v_i^n - v_j^n - v_k^n)/n \tag{3.1}$$

where $v = -2, -1, 0, 1, 2, 3,$ according to the class (Table 4).

When n is a prime, Fermat's theorem gives

$$r_i^n - r_j^n - r_k^n = r_i - r_j - r_k + nQ \tag{3.2}$$

No	Class	v_i	v_j	v_k	$(v_i - v_j - v_k)$	$v_i^n - v_j^n - v_k^n$
1	$<\overline{2},\overline{1},\overline{4}>$	-1	-2	1	0	$2^n - 2 = nT$
2	$<\overline{4},\overline{5},\overline{2}>$	1	2	-1	0	$-(2^n - 2) = -nT$
3	$<\overline{1},\overline{2},\overline{2}>$	-2	-1	-1	0	$-(2^n - 2) = -nT$
4	$<\overline{5},\overline{4},\overline{4}>$	2	1	1	0	$2^n - 2 = nT$
5	$<\overline{6},\overline{5},\overline{4}>$	3	2	1	0	$3^n - 3 - (2^n - 2) = n(S - T)$
6	$<\overline{5},\overline{2},\overline{6}>$	2	-1	3	0	$2^n - 2 - (3^n - 3) = n(T - S)$
7	$<\overline{2},\overline{3},\overline{2}>$	-1	0	-1	0	0
8	$<\overline{4},\overline{3},\overline{4}>$	1	0	1	0	0
9	$<\overline{6},\overline{1},\overline{2}>$	3	-2	-1	6	$3^n - 3 + (2^n - 2) + 6 = n(S + T) + 6$
10	$<\overline{4},\overline{1},\overline{6}>$	1	-2	3	0	$-(3^n - 3) + 2^n - 2 = n(T - S)$
11	$<\overline{1},\overline{4},\overline{6}>$	-2	1	3	-6	$-(3^n - 3) - (2^n - 2) - 6 = -n(T + S) - 6$
12	$<\overline{3},\overline{2},\overline{4}>$	0	-1	1	0	0
13	$<\overline{2},\overline{5},\overline{6}>$	-1	2	3	-6	$-(2^n - 2) - (3^n - 3) - 6 = -n(T + S) - 6$

Table 4: The v-functions

S and T are integer; $T = (2^n - 2)/n$, $S = (3^n - 3)/n$, n is a prime.

As can be seen from Table 4 the v function has n as a factor, except for the classes $<\overline{6},\overline{1},\overline{2}>$, $<\overline{1},\overline{4},\overline{6}>$ and $<\overline{2},\overline{5},\overline{6}>$ which have a residual prime to n (i.e. ± 6).

The residuals, t, will thus be of two types:

$$6(r_i - r_j - r_k)/n, \tag{3.3}$$

or

$$(6(r_i - r_j - r_k) \pm 6)/n \tag{3.4}$$

Equation (3.4) applies only to the three class sets noted above.

Substituting the components c, b and a into equations (3.3), (3.4):

$$t = (c - b - a - (v_i - v_j - v_k))/n \tag{3.5}$$

As can be seen from Table 4 and equation (3.1) the 6 of equation (3.4) will cancel out so that

$$c^n = (a + b + nt)^n \tag{3.6}$$

If $(a^n + b^n) = c^n$, the function in t is zero. Solving for t will give n roots and their value can be found as for the cubic triples.

Expanding equation (3.6) gives

$$\begin{aligned} &c^n - a^n - b^n = nQ_{ab} + n^n t^n + n^n(a+b)t^{n-1} + n^{n-1}(n-1) \\ &(a+b)^2 t^{n-2}/2 + n^{n-2}(n-1)(n-2)(a+b)^3 t^{n-3}/6 + n^{n-3} \\ &(n-1)(n-2)(n-3)(a+b)^4 t^{n-4}/24 + n^{n-4}(n-1)(n-2) \\ &(n-3)(n-4)(a+b)^5 t^{n-5}/120 \quad + ... \end{aligned} \tag{3.7}$$

If the left hand side of equation (3.7) is zero, then

$$\begin{aligned} &t^n + (a+b)t^{n-1} + (n-1)(a+b)^2 t^{n-2}/2n + (n-1)(n-2) \\ &(a+b)^3 t^{n-3}/6n^2 \ + ... \ = 0 \end{aligned} \tag{3.8}$$

This polynomial in t can have n roots, indicated by $A, B, C, D, E, ...$ Thus

$$-(a+b) = A + B + C + D + E + ... \tag{3.9}$$

$$((n-1)/2n)(a+b)^2 = AB + AC + AD + AE + ... \tag{3.10}$$

From equation (3.9)

$(a+b)^2 = (A^2 + B^2 + C^2 + D^2 + E^2 + ...) + 2(AB + AC + AD + AE + ...)$ which, when combined with equation (3.10) yields:

$$(n-1)(A^2 + B^2 + ...) = 2n(AB + AC + ...) - 2(n-1)(AB + AC + ...) \tag{3.11}$$

There are $(n-1)n/2$ terms **in** $(AB + AC + AD + ...)$ and n terms **in** $(A^2 + B^2 + C^2 + ...)$, so that, $A = B = C = ...$ would satisfy equation (3.11); that is

$$(n-1)n = 2(n-1)n/2 \tag{3.12}$$

From equation (3.9) this means that

$$A = -(a+b)/n \tag{3.13}$$

but, from equation (3.5)

$$t = (c-(b+a))/n - f(v)/n \tag{3.14}$$

and since $A \equiv t$, since all roots are the same.

$$c = f(v) \tag{3.15}$$

However $c \neq 6$ since 6 is in class $\overline{3}$ and there are no classes with c in class $\overline{3}$ that give $f(v) = 6$ (Table 4). Hence $c = 0$.

Here we have taken n as a prime. However, a number $c^{p_1 p_2 \cdots}$ may be expressed $(c^{(p_2 \cdots) p_1})$ so that above results apply generally to odd powered triples.

Appendix

The method used here is illustrated by applying it to primitive Pythagorean triples. For example take the class set $< \overline{4}\ \overline{3}\ \overline{4} >$ with

$$(6r_4 + 1)^2 = (6r_3)^2 + (6r_4' + 1)^2 \tag{A1}$$

which gives the residual t as

$$t = (r_4 - r_4')/3 \tag{A2}$$

or

$$c = a + 18t \tag{A3}$$

Squaring both sides of (A3) and putting the result in a quadratic for t form, we get:

$$t^2 + (36a/18^2)t - (b^2/(18)^2) = 0 \tag{A4}$$

If A and B are the two roots, then

$$(A + B) = -a/9 \tag{A5}$$

$$AB = -b^2/(18)^2 \tag{A6}$$

c	b	a	r_4	r_4'	$t = (r_4 - r_4')/3$	roots from eqns (A5) and (A6)
25	24	7	4	1	1	1, $-(16/9)$
-25	24	7	$-13/3$	1	$-16/9$	
205	156	133	34	22	4	4, $-(169/9)$
-205	156	133	$-103/3$	22	$-169/9$	
1381	1020	931	230	155	25	25, $-(1156/9)$
-1381	1020	931	$-691/3$	1553	$-1156/9$	

Table 5: Some examples of solutions for equations (A5) and (A6)

Unlike the odd powers greater than 2, the roots are not equal. Only one is an integer. For the given examples, the other comes from a shift of c into the negative plane.

To illustrate why the relationship

$$A^2 + B^2 + C^2 = AB + AC + BC \tag{A7}$$

implies that $A = B = C$, we assume $A = (C + \underline{a})$ and $B = (C + \underline{b})$. Substitution into equation (A7) then yields

$$(\underline{a}^2 + \underline{b}^2) = \underline{ab} \tag{A8}$$

the roots of which are imaginary, so the only solution is that both a and b are zero.

For a reasonably accessible exposition of the history of Pythagorean triples and Fermat's Last Theorem the reader is referred to van der Poorten [3], especially Lectures I and IV.

References

1. J.V. Leyendekkers, J.M. Rybak and A.G. Shannon, The anatomy of even exponent triples. *Notes on Number Theory and Discrete Mathematics,* 2, 1, 1996, 33-52.

2. J.V. Leyendekkers, J.M. Rybak and A.G. Shannon, Integer class properties associated with an integer matrix. *Notes on Number Theory and Discrete Mathematics*, 1, 2, 1995, 53-59.

3. Alf van der Poorten, *Notes on Fermat's Last Theorem*; New York: Wiley, 1996.