NNTDM 15 (2009), 4, 13-24

STRUCTURE AND SPECTRA OF THE COMPONENTS OF PRIMITIVE PYTHAGOREAN TRIPLES AND FERMAT'S LAST THEOREM

J. V. Leyendekkers
The University of Sydney, 2006, Australia

A. G. Shannon & C. K. Wong
Warrane College, The University of New South Wales, Kensington, NSW 1465, Australia

Abstract

Certain characteristics of Pythagorean triples are analysed using Integer Structure via the modular ring, Z_4. The fact (as shown by Fermat's Last Theorem) that all the components of a triple cannot simultaneously be an even power n (with $\frac{1}{2}n$ even) is illustrated via the spectra of the right-end-digits of the components.

Keywords: Pythagorean triples, right end digits, integer structure analysis modular rings

AMS Classification Numbers: 11D 41, 11A07

1. Introduction

There are many analyses in Number Theory where Integer Structure (IS) has been used to explain why certain constraints apply for various equations [3]. Here we illustrate constraints on the equation

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

With a,b,c, integers. This famous equation, a Pythagorean triple, actually underpins Fermat's Last Theorem when *n*, n/2 are even [1]. Therefore it is of interest to look at the integer structure of these triples, especially the spectra of their rows in the Modular ring z_4.

2. Structure of Pythagorean Triples

2.1 The major component c cannot be even.

Pythagorean triples have been studied throughout the many centuries following on from Pythagoras. It might seem curious that the simple equation (1.1) has the restriction that, for primitive Pythagorean triples (pPts), *c* can never be even, that is, *a* and *b* cannot both be odd.

However, this is easily explained from the integer structure [3]. We can use the modular ring z_4 to illustrate this. Within this ring the integers are given by $4r_i + i$ where $\bar{i}$ is the class and r_i the row (Table 1).

Class	$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$	Table 1
Row 0	0	1	2	3	
Row 1	4	5	6	7	
Row 2	8	9	10	11	

Note that $(4r_2 + 2)$ which represents the integers in Class $\bar{2}_4$, when raised to a power, gives an integer in Class $\bar{0}_4$, for example,

$$(4r_2 + 2)^2 = 4(4r_2^2 + 4r_2 + 1) \tag{2.1}$$

with the row in $\bar{0}_4$ equal to $(4r_2(r_2 + 1) + 1)$ which is always odd. Thus there are no powers in Class $\bar{2}_4$. When integers in Class $\bar{3}_4$ are raised to an even power the resultant integer always falls in Class $\bar{1}_4$, for example

$$(4r_3 + 3)^2 = 4(4r_3 + 6r_3 + 2) + 1 \tag{2.2}$$

with the row given by $(4r_3 + 6r_3 + 2)$ which is always even. Thus there are no even powers in Class $\bar{3}_4$. With these constraints, we have

$$\bar{1}_4 + \bar{1}_4 = \bar{2}_4 \tag{2.3}$$

Thus, since the odd squares always fall in Class $\bar{1}_4$ their sum must fall in Class $\bar{2}_4$ but this class has no powers, so the triple cannot be formed.

2.2 The even component can never fall in class $\bar{2}_4$

This is another restriction that is easily explained using IS. Since

$$(4r_1 + 1)^2 + (4r_2 + 2)^2 = 4(4(r_1^2 + r_2^2) + 2(r_1 + 2r_2) + 1) + 1 \tag{2.4}$$

$$\text{or } (4r_3 + 3)^2 + (4r_2 + 2)^2 = 4(4(r_3^2 + r_2^2) + 6r_3 + 4r_2 + 3) + 1 \tag{2.5}$$

This means that the row of the resultant integer from the summed squares must be odd. However, squares in class $\bar{1}_4$ have rows that are always even, for example

$$(4r_1 + 1)^2 = 4(4r_1^2 + 2r_1) + 1 \tag{2.6}$$

Which has an even row, or

$$(4r_3 + 3)^2 = 4(4r_3^2 + 6r_3 + 2) + 1 \tag{2.7}$$

Which also has an even row. Hence the even component of a pPt can never fall in class $\bar{2}_4$.

2.3 Row structure of triples.

Triples of the form (*c*,*b*,*a*) ε $\bar{1}_4\bar{0}_4\bar{3}_4$ have the rows of their squares in classes $\bar{2}_4\bar{0}_4\bar{2}_4$ (when the rows of $\bar{3}_4$ integers are even) or in class $\bar{0}_4\bar{0}_4\bar{0}_4$ (when rows of $\bar{3}_4$ integers are odd).

Triples of the form $\bar{1}_4\bar{0}_4\bar{1}_4$ have the rows of their squares in classes $\bar{2}_4\bar{0}_4\bar{2}_4$ (when rows of *a* are odd) or in $\bar{0}_4\bar{0}_4\bar{0}_4$ (when rows of *a* are even). The class structure of the row of the row of (c^2, b^2, a^2) is more diverse (Table 2)

Triples	R_i † Classes
$\bar{1}_4\bar{0}_4\bar{3}_4$	$\bar{0}_4\bar{0}_4\bar{0}_4$
	$\bar{1}_4\bar{1}_4\bar{0}_4$
	$\bar{3}_4\bar{0}_4\bar{3}_4$
	$\bar{2}_4\bar{0}_4\bar{2}_4$
	$\bar{1}_4\bar{0}_4\bar{1}_4$
$\bar{1}_4\bar{0}_4\bar{1}_4$	$\bar{0}_4\bar{0}_4\bar{0}_4$
	$\bar{3}_4\bar{1}_4\bar{2}_4$
	$\bar{0}_4\bar{1}_4\bar{3}_4$
	$\bar{2}_4\bar{1}_4\bar{1}_4$
	$\bar{1}_4\bar{0}_4\bar{1}_4$
Table 2: † R_i represents the rows of the rows of (c^2, b^2, a^2)	

Note that the row of b^2 (the even component here) always falls in $\bar{0}_4$. In general, the rows of even squares are themselves squares, an important feature, as will be shown below.

2.4 The Largest Component, *c,* is $3 \nmid c$.

Another interesting feature of pPts is that the largest component, *c*, has no factors in 3. This can be understood as follows. Since *c* ε $\bar{1}_4$, *c* may be a sum of squares. In fact, *c* must be a sum of squares. This is shown via the (*z*-*j*) grid analysis of pPts [3] whereby with $c > b > a$ and $z = c - b$:

$$c = j_o^2 + (j_o + z_o^{\frac{1}{2}})^2 \tag{2.8}$$

with *z* odd, and

$$(z_o = (2t-1)^2)$$

or

$$c = ((\frac{1}{2}z_e)^{\frac{1}{2}})^2 + ((\frac{1}{2}z_e)^{\frac{1}{2}} + (2j_e - 1))^2 \tag{2.9}$$

with *z* even, and

$$z_e = 2t^2.$$

Some examples are shown in Table 3

pPt	z_o	j_o	$j_o + z_o^{\frac{1}{2}}$	Table 3.
233,208,165	25	8	13	
65,56,33	9	4	7	
137,88,105	49	4	11	
169,120,119	49	5	12	

Not all integers in Class $\bar{1}_4$ are a sum of squares since many contain factors that derive from Class $\bar{\bar{3}}_4$. Sums of squares do not occur in this Class [3]. For example, if 3 is a factor, $3\varepsilon\,\bar{\bar{3}}_4$ and hence sums of squares do not occur. For example 21, 33, 81 are in Class $\bar{1}_4$ but do not equal a sum of squares since the factors 3x7, 3x11 and 3x3x3x3 fall in $\bar{\bar{3}}_4$. Hence any integers in Class $\bar{1}_4$ that do not equal a sum of squares cannot be the major component of a pPt.

3. Can the components of a pPt all be squares?

Obviously, since Class $\bar{\bar{3}}_4$ contains no even powers the pPt class structure $\bar{1}_4\bar{0}_4\bar{\bar{3}}_4$ would not apply and only $\bar{1}_4\bar{0}_4\bar{1}_4$ need be considered. The rows of squares are well characterised and an analysis using this information shows that all components (*c,b,a*) of a pPt cannot be squares [3].

Here we take a more visual approach and look at the right-end digits (REDs) of the rows of the components and compare them to the REDs of rows of squares. Spectra of the REDs of rows of the components of a pPt illustrate how repeat sequences simplify comparisons (Figures 1 to 8).

A range of pPts and their rows in z_4 were calculated for various odd *z*. Table 4 lists the REDs of the rows. REDs are indicated by a superscript asterisk. Furthermore, the REDs of the rows were plotted to form spectra of the different components. These spectra consisted of repeat sequences covering *j* values up to around 20 for *c* and *b* but only a small number of *j* for component *a* (Figures 1-8).

Note that we have taken *z* odd here, that is *b*, the second largest component, is even. The reader might like to explore the spectra when z is even (second largest component is odd). The REDs are summarised in Table 4 where a tick indicates that a RED is compatible with the REDs of squares, whereas a cross indicates incompatibility.

Remarkably, in the basic units (which are repeated and hence represent the overall structure) there are only one or two sets that appear to be compatible with squares. These few deviants are easily disposed of (since $r_b^* = 0$ can be converted to a cross). This is because the rows of even squares must be squares. Thus the row of the row of component b must have a RED compatible with a square.

Table 4: REDs of the rows of c, b and a												
z=1			z=9			z=25			z=49			
r_c^*	r_b^*	r_a^*	r_c^*	r_b^*	r_a^*	r_c^*	r_b^*	r_a^*	r_c^*	r_b^*	r_a^*	
$1^{\times}$	$1^{\checkmark}$	$0^{\checkmark}$	$1^{\times}$	$9^{\checkmark}$	$6^{\checkmark}$	$4^{\times}$	$8^{\times}$	$6^{\checkmark}$	$2^{\checkmark}$	$0^{\checkmark}$	$9^{\times}$	
$3^{\times}$	$3^{\times}$	$1^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$8^{\times}$	$1^{\times}$	$5^{\checkmark}$	$8^{\times}$	$1^{\times}$	$9^{\checkmark}$	$3^{\times}$	
$6^{\checkmark}$	$6^{\checkmark}$	$1^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$9^{\times}$	$9^{\times}$	$3^{\times}$	$1^{\checkmark}$	$1^{\times}$	$9^{\checkmark}$	$6^{\checkmark}$	
$0^{\checkmark}$	$0^{\checkmark}$	$2^{\checkmark}$	$9^{\times}$	$7^{\times}$	$1^{\times}$	$8^{\times}$	$2^{\times}$	$3^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$0^{\checkmark}$	
$5^{\times}$	$5^{\checkmark}$	$2^{\checkmark}$	$7^{\times}$	$5^{\checkmark}$	$2^{\checkmark}$	$8^{\times}$	$2^{\times}$	$6^{\checkmark}$	$4^{\times}$	$2^{\times}$	$3^{\times}$	
$1^{\times}$	$1^{\checkmark}$	$3^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$4^{\times}$	$9^{\times}$	$3^{\times}$	$8^{\times}$	$7^{\times}$	$5^{\checkmark}$	$7^{\times}$	
$8^{\times}$	$8^{\times}$	$3^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$5^{\times}$	$1^{\times}$	$5^{\checkmark}$	$1^{\times}$	$1^{\times}$	$9^{\checkmark}$	$0^{\checkmark}$	
$6^{\checkmark}$	$6^{\checkmark}$	$4^{\times}$	$7^{\times}$	$5^{\checkmark}$	$7^{\times}$	$4^{\times}$	$8^{\times}$	$3^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$4^{\times}$	
$5^{\times}$	$5^{\checkmark}$	$4^{\times}$	$9^{\times}$	$7^{\times}$	$8^{\times}$	$8^{\times}$	$2^{\times}$	$6^{\checkmark}$	$2^{\checkmark}$	$0^{\checkmark}$	$7^{\times}$	
$5^{\times}$	$5^{\checkmark}$	$5^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$0^{\checkmark}$	$3^{\times}$	$7^{\times}$	$8^{\times}$	$9^{\times}$	$7^{\times}$	$1^{\times}$	
$6^{\checkmark}$	$6^{\checkmark}$	$5^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$1^{\times}$	$9^{\times}$	$3^{\times}$	$1^{\times}$	$7^{\times}$	$5^{\checkmark}$	$4^{\times}$	
$8^{\times}$	$8^{\times}$	$6^{\checkmark}$	$1^{\times}$	$9^{\checkmark}$	$3^{\times}$	$6^{\checkmark}$	$0^{\checkmark}$	$3^{\times}$	$6^{\checkmark}$	$5^{\checkmark}$	$8^{\times}$	
$1^{\times}$	$1^{\checkmark}$	$6^{\checkmark}$	$7^{\times}$	$5^{\checkmark}$	$4^{\times}$	$4^{\times}$	$8^{\times}$	$6^{\checkmark}$	$6^{\checkmark}$	$4^{\checkmark}$	$1^{\times}$	
$5^{\times}$	$5^{\checkmark}$	$7^{\times}$	$4^{\times}$	$2^{\times}$	$6^{\checkmark}$	$3^{\times}$	$7^{\times}$	$8^{\times}$	$7^{\times}$	$5^{\checkmark}$	$5^{\times}$	
$0^{\checkmark}$	$0^{\checkmark}$	$7^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$7^{\times}$	$3^{\times}$	$7^{\times}$	$1^{\times}$	$9^{\times}$	$7^{\times}$	$8^{\times}$	
$6^{\checkmark}$	$6^{\checkmark}$	$8^{\times}$	$1^{\times}$	$9^{\checkmark}$	$9^{\times}$	$4^{\times}$	$8^{\times}$	$3^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$2^{\checkmark}$	
$3^{\times}$	$3^{\times}$	$8^{\times}$	$1^{\times}$	$9^{\checkmark}$	$0^{\checkmark}$	$6^{\checkmark}$	$0^{\checkmark}$	$6^{\checkmark}$	$6^{\checkmark}$	$4^{\checkmark}$	$5^{\times}$	
$1^{\times}$	$1^{\checkmark}$	$9^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$2^{\checkmark}$	$9^{\times}$	$3^{\times}$	$8^{\times}$	$1^{\times}$	$9^{\checkmark}$	$9^{\checkmark}$	
$0^{\checkmark}$	$0^{\checkmark}$	$9^{\times}$	$4^{\times}$	$2^{\times}$	$3^{\times}$	$3^{\times}$	$7^{\times}$	$1^{\times}$	$7^{\times}$	$5^{\checkmark}$	$2^{\checkmark}$	
$0^{\checkmark}$	$0^{\checkmark}$	$0^{\checkmark}$	$7^{\times}$	$5^{\checkmark}$	$5^{\times}$	$8^{\times}$	$2^{\times}$	$3^{\times}$	$4^{\times}$	$2^{\times}$	$6^{\checkmark}$	
$1^{\times}$	$1^{\checkmark}$	$0^{\checkmark}$	$1^{\times}$	$9^{\checkmark}$	$6^{\checkmark}$	$4^{\times}$	$8^{\times}$	$6^{\checkmark}$	$2^{\checkmark}$	$0^{\checkmark}$	$9^{\times}$	
$3^{\times}$	$3^{\times}$	$1^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$8^{\times}$	$1^{\times}$	$5^{\checkmark}$	$8^{\times}$	$1^{\times}$	$9^{\checkmark}$	$3^{\times}$	
$6^{\checkmark}$	$6^{\checkmark}$	$1^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$9^{\times}$	$9^{\times}$	$3^{\times}$	$1^{\times}$	$1^{\times}$	$9^{\checkmark}$	$6^{\checkmark}$	
$0^{\checkmark}$	$0^{\checkmark}$	$2^{\checkmark}$	$9^{\times}$	$7^{\times}$	$1^{\times}$	$8^{\times}$	$2^{\times}$	$3^{\times}$	$2^{\checkmark}$	$0^{\checkmark}$	$0^{\checkmark}$	
$5^{\times}$	$5^{\checkmark}$	$2^{\checkmark}$	$7^{\times}$	$5^{\checkmark}$	$2^{\checkmark}$	$8^{\times}$	$2^{\times}$	$6^{\checkmark}$	$4^{\times}$	$2^{\times}$	$3^{\times}$	
$1^{\times}$	$1^{\checkmark}$	$3^{\times}$	$6^{\checkmark}$	$4^{\checkmark}$	$4^{\times}$	$9^{\times}$	$3^{\times}$	$8^{\times}$	$7^{\times}$	$5^{\checkmark}$	$7^{\times}$	

Table 5 shows that this is not the case. For z = 49 the row of r_b^* is consistent with a square, however the RED of the row of the row of r_b^* is not since it should be even.

Table 5.				
z	j	r_b^*	row of r_b^*	row of row of r_b^*
1	4	0	2	
	20	0	2	
9	12	0	2	
	20	0	7	
25	20	0	2	
49	8	0	5	3
	20	0	7	

4. Final Comments

As has been discussed before [3], the truth of Fermat's Last Theorem conforms with the structure of integers as shown by modular rings (in this case z_4), does not contain a row to fit the sum of two identical powers into the same power slot in the ring. Here we have illustrated this for the case of *n* and *n*/2 being even. Finally the interested reader might like to explore the links between IS and the Artin-Schreier [2] theory to the effect that "fundamental theorem of algebra truly is an algebraic theorem inasmuch as it states that all irreducible polynomials over real closed fields can only be linear or quadratic" [4].

5. References

1. Aczel, Amir D. 1997. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem.* New York: Delta.
2. Artin, Emil. Otto Schreier. Algebraische Konstruktion reeler Körper. *Abhandlungen aus dem Mathematichen Seminar der Universität Hamburg*. 5, 1927:85-99.
3. Leyendekkers, J.V., A.G. Shannon, J.M. Rybak. *Pattern Recognition: Modular Rings and Integer Structure.* North Sydney: Raffles KvB Monograph No.9, 2007.
4. Zassenchaus, H., Emil Artin. His Life and Work. *Notre Dame Journal of Formal Logic*. 5, 1964: 1-9

Figure 1. (z=1)

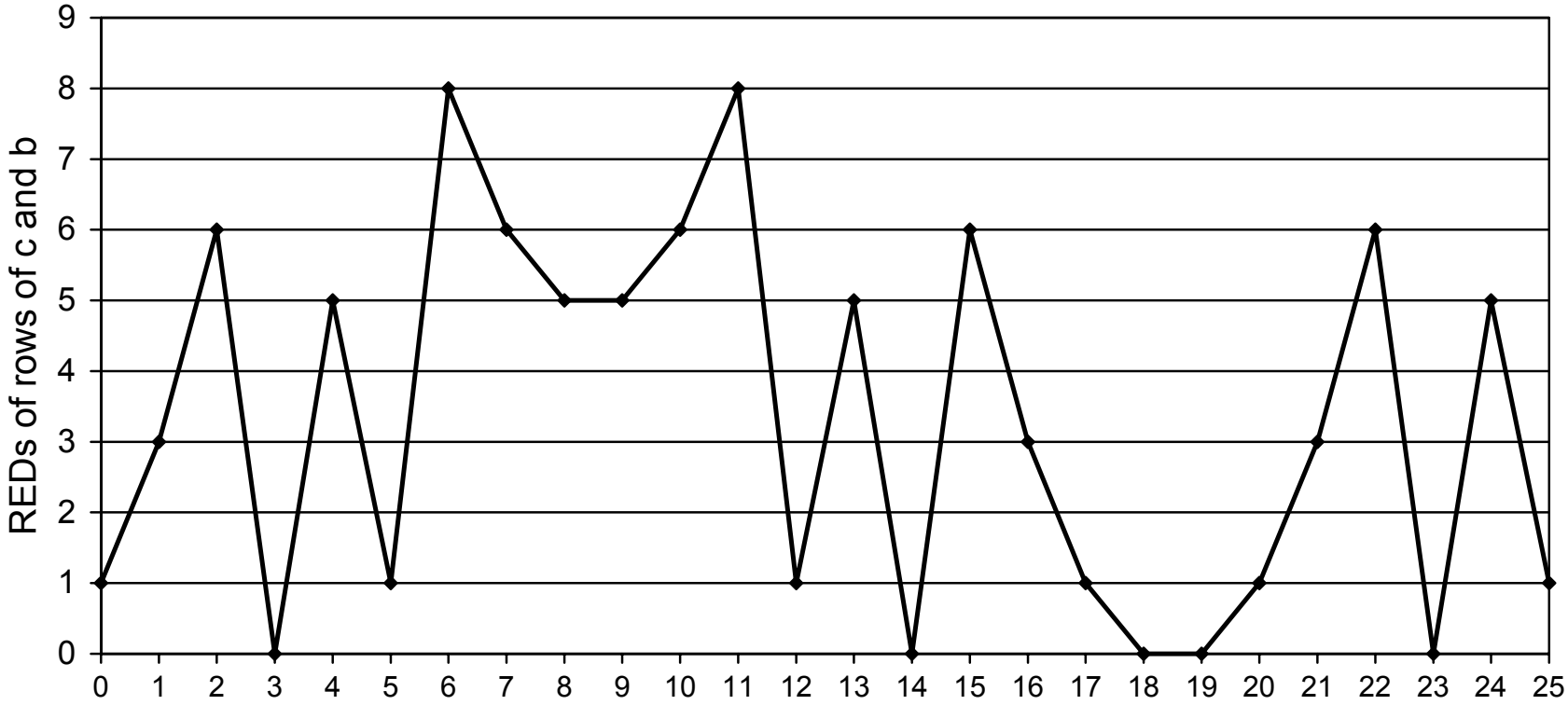
REDs of rows of c and b
0
1
2
3
4
5
6
7
8
9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Figure 2. (z=1)

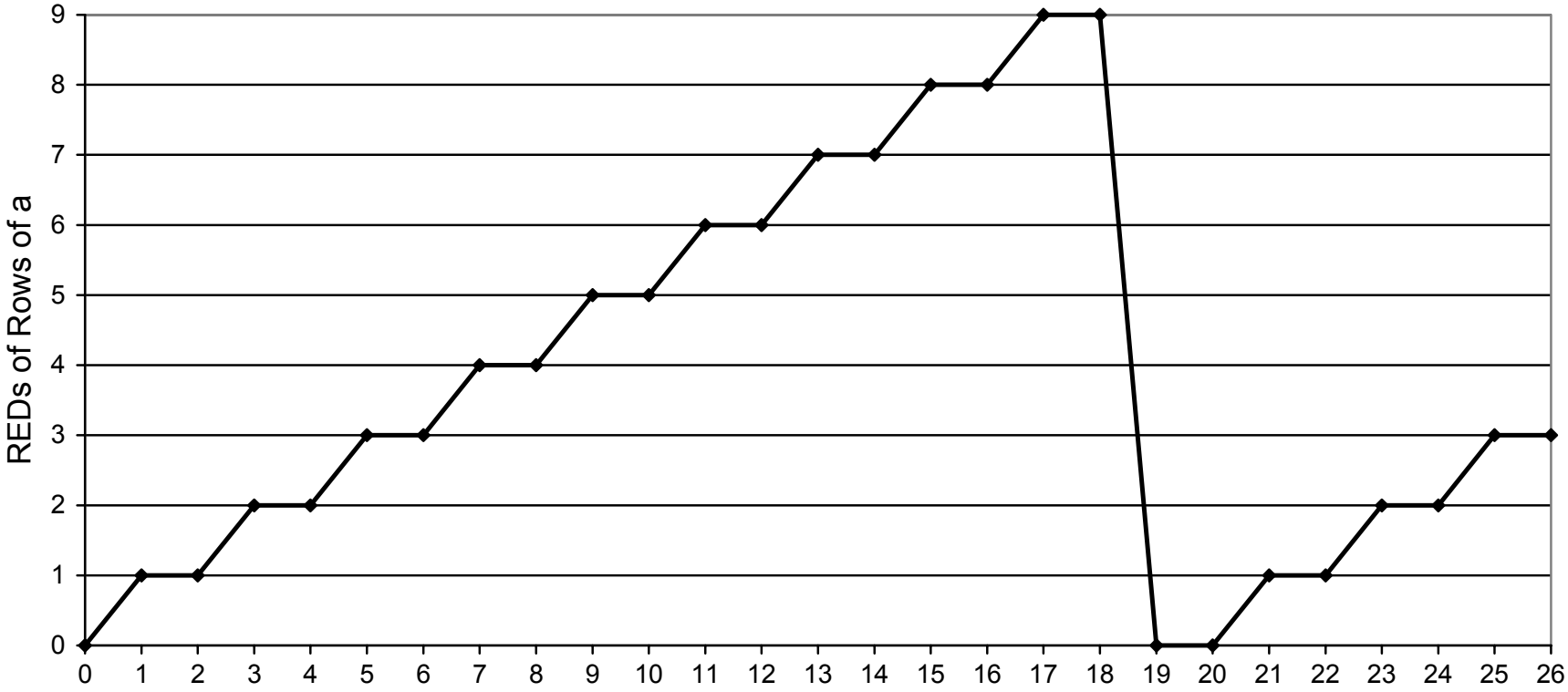
REDs of Rows of a
0
1
2
3
4
5
6
7
8
9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Figure 3. (z=9)

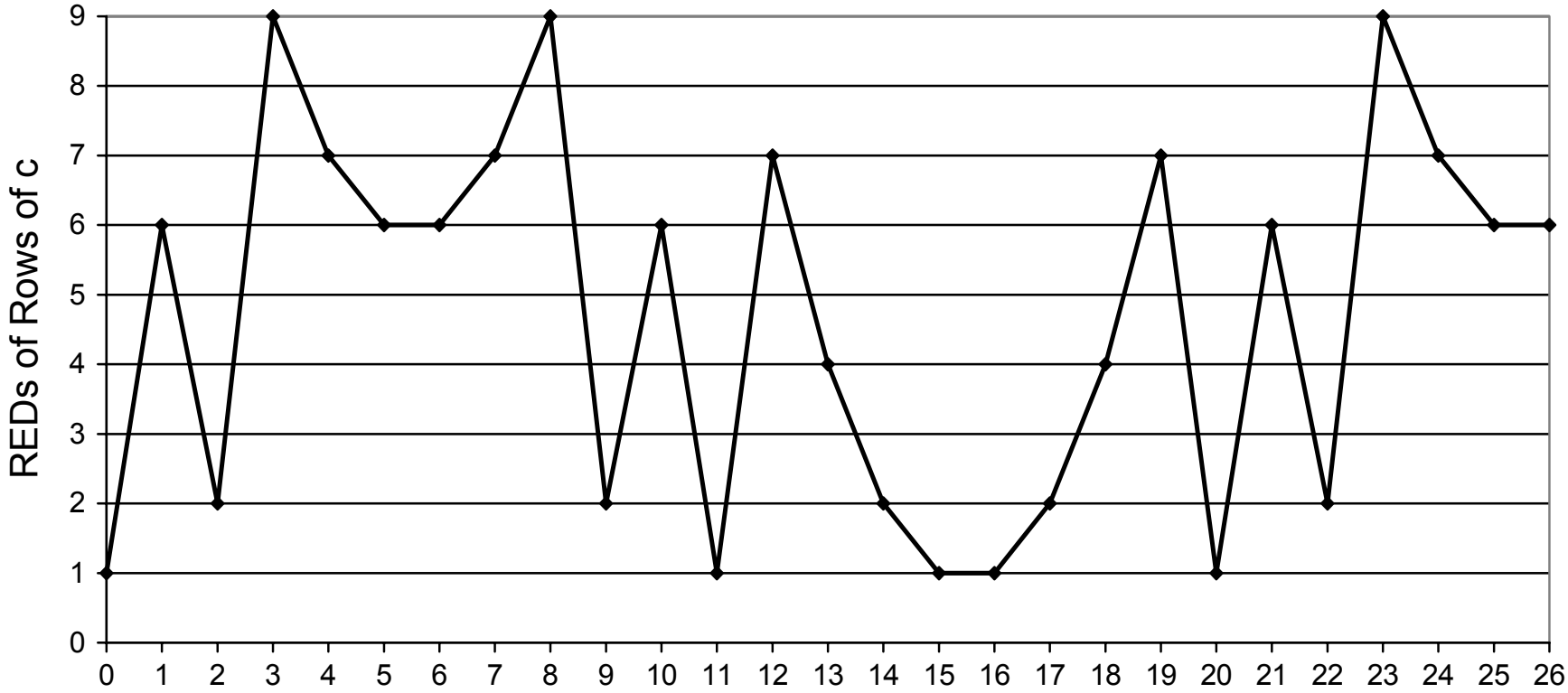
REDs of Rows of c
0
1
2
3
4
5
6
7
8
9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Figure 4. (z=9)

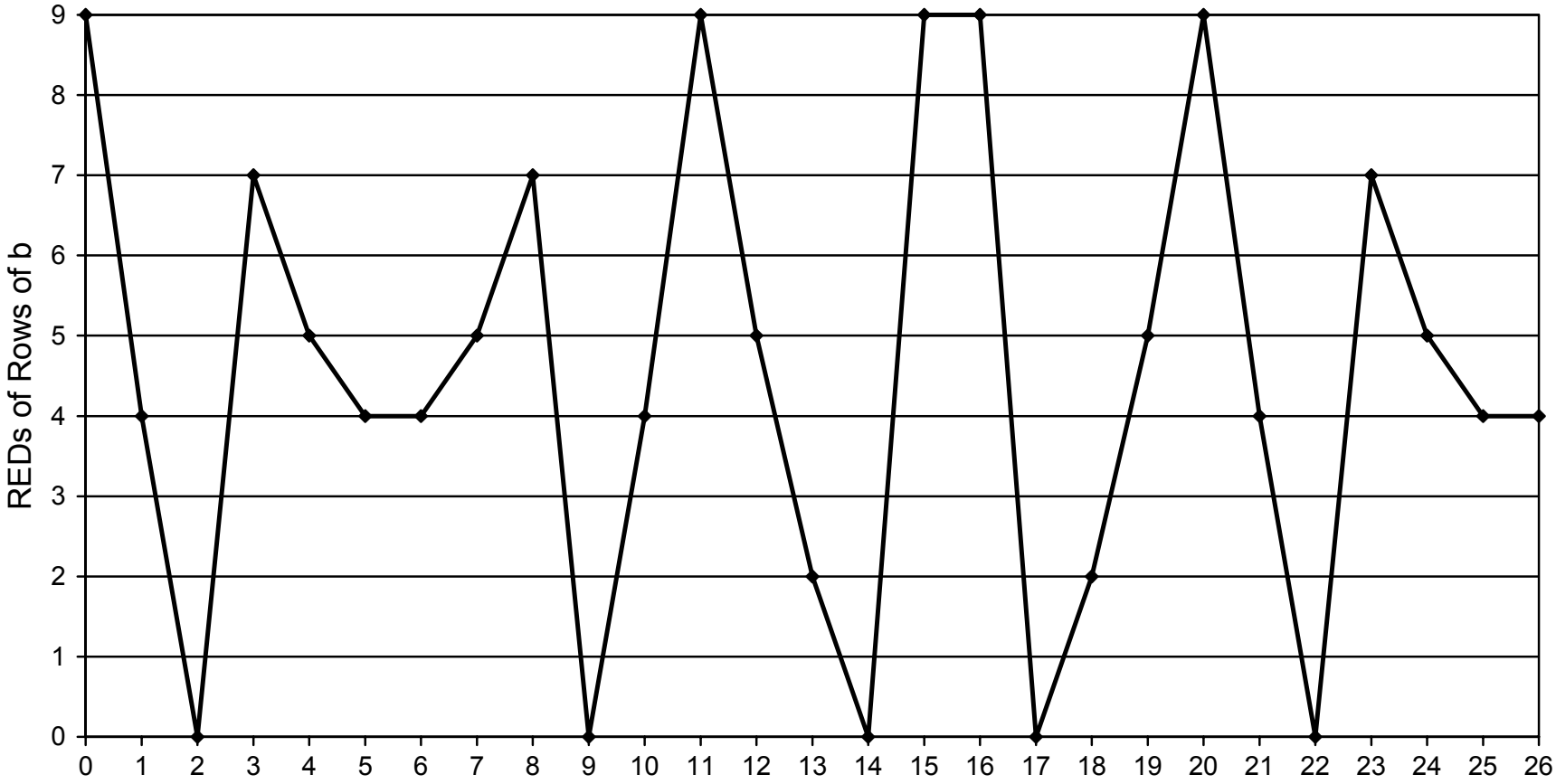
REDs of Rows of b
0
1
2
3
4
5
6
7
8
9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Figure 5. (z=9)

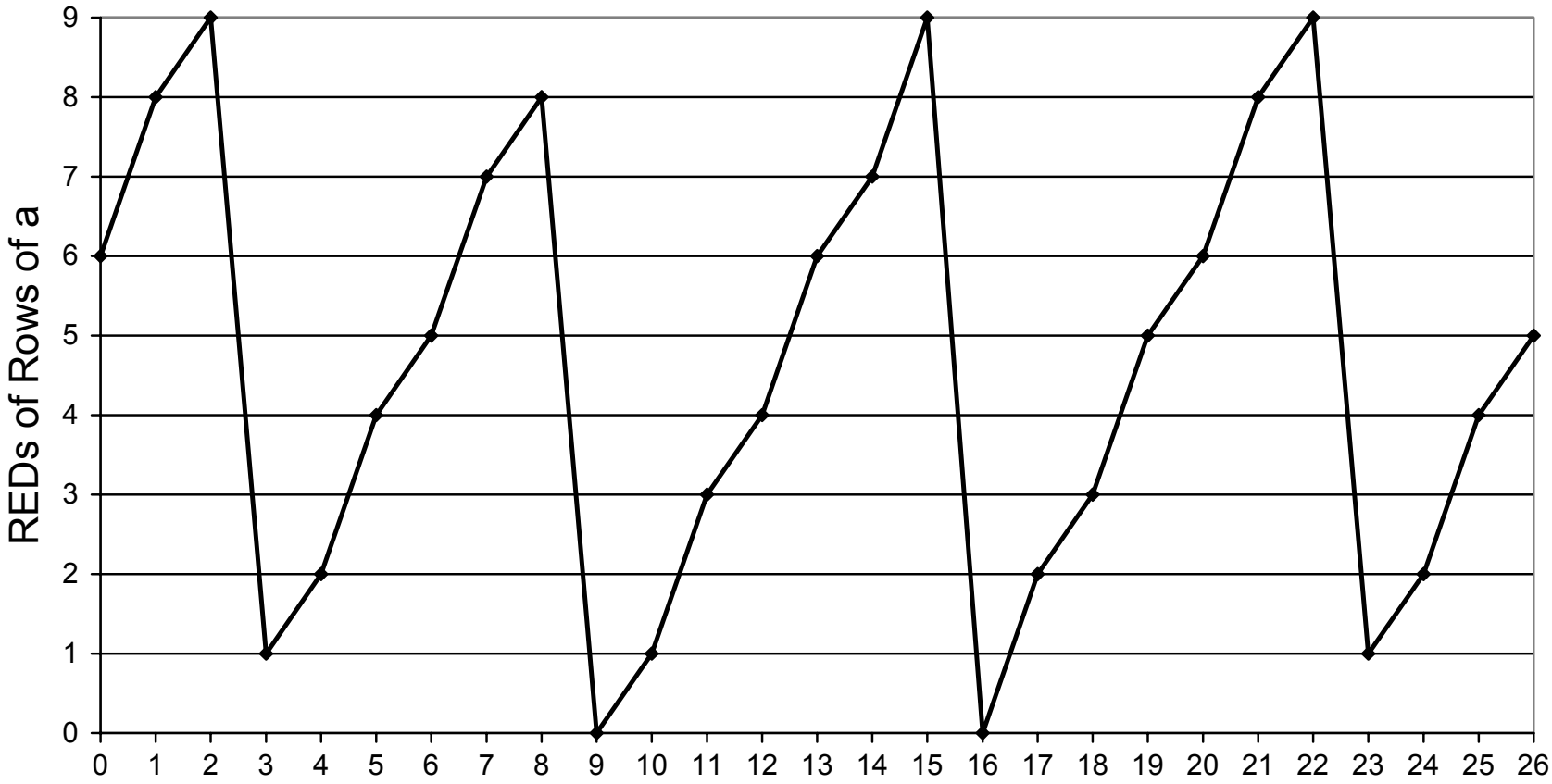
REDs of Rows of a
0
1
2
3
4
5
6
7
8
9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Figure 6. (z=25)

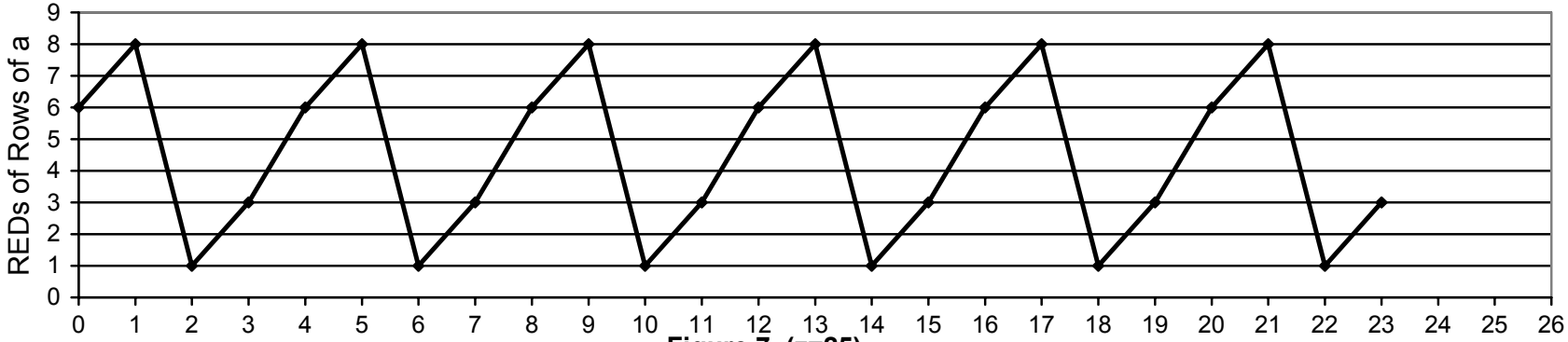

Figure 7. (z=25)

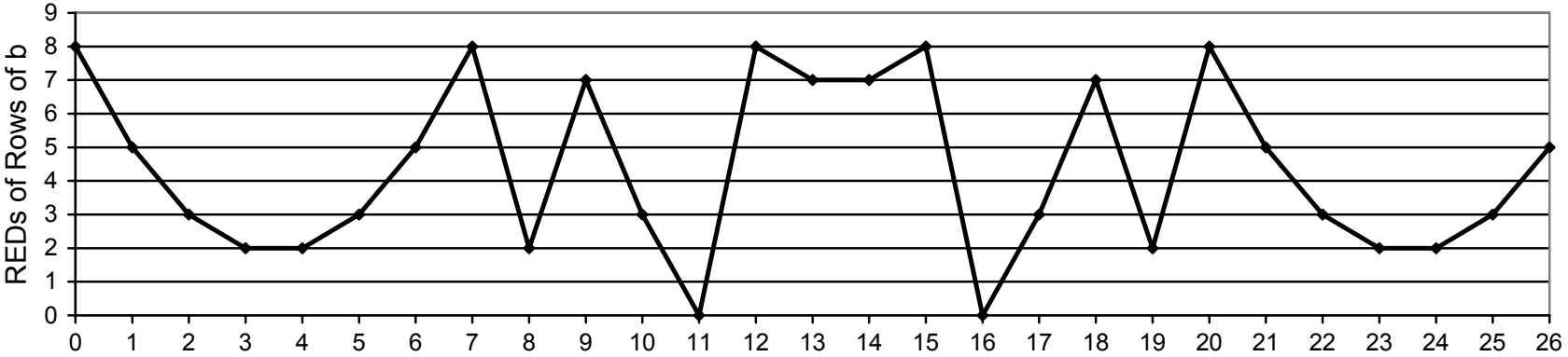

Figure 8. (z=25)