NNTDM 12 (2006), 3, 10-19

USING INTEGER STRUCTURE TO SOLVE DIOPHANTINE EQUATIONS

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

A. G. Shannon
Warrane College, The University of New South Wales, Kensington, 1465,
& KB Institute of Technology, North Sydney, NSW 2060, Australia

Abstract

Diophantine equations $\{ax + by = c; a, b, c \in Z\}$ are classified according to parity constraints. Various types, so classified, are solved with the theory of integer structure, via the modular ring Z_4. The simplest forms are those where one of the variables is confined to a single class. However, the more complex equations have solutions that follow regular (*x*,*y*) class patterns. The famous Diophantine equation in Fermat's Last Theorem is discussed in terms of the factor structure of the sum of two powers.

1. Introduction

Diophantine equations date back thousands of years and have the form

$$ax + by = c,\ abc \in Z. \tag{1.1}$$

These equations have integer solutions iff $(a,b)|c$ [7]. Euclid's algorithm and continued fractions are commonly used to solve them. In this paper we utilise integer structure so that not only can solutions be identified but also different forms of the solutions.

To do this we use the modular ring Z_4 in which integers are represented by $(4r_i + \bar{i})$ in which $\bar{i}$ is the class. Thus even integers are represented by $4r_0 \in \bar{0}_4$ and $(4r_2 + 2) \in \bar{2}_4$; the latter has no powers since $(4r_2 + 2)^n \in \bar{0}_4$, n>1. Odd integers have the forms $(4r_1 + 1) \in \bar{1}_4$ and $(4r_3 + 3) \in \bar{3}_4$; the latter has no even powers since $(4r_3 + 3)^{2n} \in \bar{1}_4$ so it has no integers as a sum of squares.

Number	*a*	*b*	*c*	*x*	*y*
1	e	o	o	e or o	o
2	e	o	e	e or o	e
3	o	e	e	e	e or o
4	o	e	o	o	e or o
5	o	o	e	e o	e o
6	o	o	o	e	o

				o	e

Table 1: Parity constraints

It is only necessary to find one integer solution of Equation (1.1) as it is well known that the others depend on *a* and *b* [1]. Table 1 shows the parity constraints on *x* and *y* for a given set {*a*,*b*,*c*}: o ≡ 'odd'; e ≡ 'even'.

2. Examples of Various Sets from Table 1

Set 1. Consider the equation

$$8x + 3y = 91. \tag{2.1}$$

From Table 1, *x* is even or odd, but *y* is always odd. $c \in \bar{3}_4$ (4x22+3) so that the left hand side of Equation (2.1) must be in the same class. The possible combinations are listed in Table 2.

Number	*x*	*y*	*ax*+*by*
1	$\bar{0}_4$	$\bar{3}_4$	$\bar{0}_4 \times \bar{0}_4 + \bar{3}_4 \times \bar{3}_4 = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$
2	$\bar{0}_4$	$\bar{1}_4$	$\bar{0}_4 \times \bar{0}_4 + \bar{1}_4 \times \bar{3}_4 = \bar{3}_4 + \bar{0}_4 = \bar{3}_4$
3	$\bar{2}_4$	$\bar{3}_4$	$\bar{0}_4 \times \bar{2}_4 + \bar{3}_4 \times \bar{3}_4 = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$
4	$\bar{2}_4$	$\bar{1}_4$	$\bar{0}_4 \times \bar{2}_4 + \bar{3}_4 \times \bar{1}_4 = \bar{0}_4 + \bar{3}_4 = \bar{3}_4$
5	$\bar{1}_4$	$\bar{3}_4$	$\bar{0}_4 \times \bar{1}_4 + \bar{3}_4 \times \bar{3}_4 = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$
6	$\bar{1}_4$	$\bar{1}_4$	$\bar{0}_4 \times \bar{1}_4 + \bar{3}_4 \times \bar{1}_4 = \bar{0}_4 + \bar{3}_4 = \bar{3}_4$
7	$\bar{3}_4$	$\bar{3}_4$	$\bar{0}_4 \times \bar{3}_4 + \bar{3}_4 \times \bar{3}_4 = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$
8	$\bar{3}_4$	$\bar{1}_4$	$\bar{0}_4 \times \bar{3}_4 + \bar{3}_4 \times \bar{1}_4 = \bar{0}_4 + \bar{3}_4 = \bar{3}_4$

Table 2: Classes for Equation (2.1)

Notice that $\bar{3}_4$ has no even powers so that $\bar{3}_4 \times \bar{3}_4 = \bar{1}_4$. Also $a \in \bar{0}_4$ and $b \in \bar{3}_4$. Obviously the only valid class for *y* is $\bar{1}_4$. Thus from Equation (2.1), r_1 must be even because

$$\begin{aligned} x &= \tfrac{1}{8}(91 - 3(4r_1 + 1)) \\ &= 11 - \tfrac{3}{2} r_1. \end{aligned} \tag{2.2}$$

With $r_1 = 2, x = 8, y = 9$. All other solutions for *x* will change by *b*, that is 3, (*x*=20,17,14, 11,8,5,2,-1,-4), while *y* will change by *a*, that is 8, (*y*=-23,-15,-7,1,9,17,25,33,47). Since *y* is restricted to the one class we are able to use the class function for *y*, whereas *x* is unrestricted in terms of class and is kept as a free variable.

Set 3. Consider the equation

$$89x - 244y = 64. \tag{2.3}$$

Here *x* is always even so the class function is used for *x*: $89 \in \bar{1}_4, 244 \in \bar{0}_4, c \in \bar{0}_4$.

Since 244*y* and $64 \in \bar{0}_4, 89x \in \bar{0}_4$. In other words, $x \in \bar{0}_4$. Thus,

$$y = \tfrac{1}{61}(89r_0 - 16). \tag{2.4}$$

When $r_0 = 18, y = 26$. Thus $x_1 = 72, x_2 = 72 + 244 = 316, y_2 = 26 + 89 = 115$, and so on.

Set 4. Consider the equation

$$3x + 4y = 17. \tag{2.5}$$

For this set, x must be odd, but y can be even or odd. $17 \in \bar{1}_4, a \in \bar{3}_4, b \in \bar{0}_4$. The permissible combinations are set out in Table 3.

Number	x	y	$ax+by$
1	$\bar{1}_4$	$\bar{0}_4$	$\bar{3}_4 \times \bar{1}_4 + \bar{0}_4 \times \bar{0}_4 = \bar{3}_4$
2	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4 \times \bar{1}_4 + \bar{0}_4 \times \bar{2}_4 = \bar{3}_4$
3	$\bar{1}_4$	$\bar{1}_4$	$\bar{3}_4 \times \bar{1}_4 + \bar{0}_4 \times \bar{1}_4 = \bar{3}_4$
4	$\bar{1}_4$	$\bar{3}_4$	$\bar{3}_4 \times \bar{1}_4 + \bar{0}_4 \times \bar{3}_4 = \bar{3}_4$
5	$\bar{3}_4$	$\bar{0}_4$	$\bar{3}_4 \times \bar{3}_4 + 0_4 \times 0_4 = \bar{1}_4$
6	$\bar{3}_4$	$\bar{2}_4$	$\bar{3}_4 \times \bar{3}_4 + \bar{0}_4 \times \bar{2}_4 = \bar{1}_4$
7	$\bar{3}_4$	$\bar{1}_4$	$\bar{3}_4 \times \bar{3}_4 = \bar{0}_4 + \bar{1}_4 = \bar{1}_4$
8	$\bar{3}_4$	$\bar{3}_4$	$\bar{3}_4 \times \bar{3}_4 + \bar{0}_4 \times 3_4 = \bar{1}_4$

Table 3: Classes for Equation (2.5)

Permissible values of x are confined to $\bar{3}_4$ since $a \in \bar{3}_4$ and $b \in \bar{0}_4$. Thus $\bar{3}_4$ must be multiplied by $\bar{3}_4$ to get $\bar{1}_4$ ($3x$) and class $\bar{0}_4$ multiplied by any other class always yields $\bar{0}_4$ ($4y$). Thus, Equation (2.5) becomes:

$$3(4r_3 + 3) + 4y = 17 \tag{2.6}$$

$$y = 2 - 3r_3. \tag{2.7}$$

When $r_3 = 0$, y=2 and x=3. All subsequent x change by ± 4 while the corresponding y change by ∓ 3. For example, (x,y) = {(-21,20),(-17,17),(-13,14),(-9,11),(-5,8),(-1,5),(3,2), (7,-1),(11,-4),(15,-7),…}.

Number	x	y	$ax+by$
1	$\bar{3}_4$	$\bar{3}_4$	$\bar{1}_4 \times \bar{3}_4 - \bar{3}_4 \times \bar{3}_4 = \bar{3}_4 - \bar{1}_4 = \bar{2}_4$
2	$\bar{1}_4$	$\bar{1}_4$	$\bar{1}_4 \times \bar{1}_4 - \bar{3}_4 \times \bar{1}_4 = \bar{1}_4 - \bar{3}_4 = \bar{2}_4$
3	$\bar{3}_4$	$\bar{1}_4$	$\bar{1}_4 \times \bar{3}_4 - \bar{3}_4 \times \bar{1}_4 = \bar{3}_4 - \bar{3}_4 = \bar{0}_4$
4	$\bar{1}_4$	$\bar{3}_4$	$\bar{1}_4 \times \bar{1}_4 - \bar{3}_4 \times \bar{3}_4 = \bar{1}_4 - \bar{1}_4 = \bar{0}_4$
5	$\bar{0}_4$	$\bar{0}_4$	$\bar{1}_4 \times \bar{0}_4 - \bar{3}_4 \times \bar{0}_4 = \bar{0}_4 - \bar{0}_4 = \bar{0}_4$
6	$\bar{0}_4$	$\bar{2}_4$	$\bar{1}_4 \times \bar{0}_4 - \bar{3}_4 \times \bar{2}_4 = \bar{0}_4 - \bar{2}_4 = \bar{2}_4$
7	$\bar{2}_4$	$\bar{0}_4$	$\bar{1}_4 \times \bar{2}_4 - \bar{3}_4 \times \bar{0}_4 = \bar{2}_4 - \bar{0}_4 = \bar{2}_4$
8	$\bar{2}_4$	$\bar{2}_4$	$\bar{1}_4 \times \bar{2}_4 - \bar{3}_4 \times \bar{2}_4 = \bar{2}_4 - \bar{2}_4 = \bar{0}_4$

Table 4: Classes for Equation (2.8)

Set 5. Consider the equation

$$89x - 243y = 6. \tag{2.8}$$

This set is interesting because neither x nor y is confined to one parity, although they must both have the same parity. $c = 6 \in \bar{2}_4 \Rightarrow (ax - by) \in \bar{2}_4 : a = 89 \in \bar{1}_4, b = 243 \in \bar{3}_4$. Table 4 lists permissible classes for x and y.

From this table, it can be seen that the permissible class couples for (x,y) are:

$$(\bar{3}_4, \bar{3}_4), (\bar{1}_4, \bar{1}_4), (\bar{0}_4, \bar{2}_4), (\bar{2}_4, \bar{0}_4).$$

For $(\bar{3}_4, \bar{3}_4)$, Equation (2.8) becomes

$$89(4r_3 + 3) - 243(4r_3' + 3) = 6. \tag{2.9}$$

The first integer solution occurs for $r_3' = 16, r_3 = 45,$ to yield (x,y)=(183,67). Since x<243, this is the first member of the positive series for (x,y). The following members, $(x_1 + b, y_1 + c)$ are listed in Table 5 with the relevant class couples. These follow a regular class pattern as might be expected.

x	y	Class Structure
183	67	$(\bar{3}_4, \bar{3}_4)$
426	156	$(\bar{2}_4 \bar{0}_4)$
669	245	$(\bar{1}_4, \bar{1}_4)$
912	334	$(\bar{0}_4, \bar{2}_4)$
1155	423	$(\bar{3}_4, \bar{3}_4)$
1398	512	$(\bar{2}_4 \bar{0}_4)$

Table 5: Results for Equation (2.9)

3. Fermat's Last Theorem

Since Fermat wrote his famous statement on his so-called "Last Theorem" in the margin of his edition of Diophantus (Toulouse, 1670, bk.II, qn.8, p.61), it can be assumed that the Diophantine equations either inspired or formed the basis of his general theorem. For example, suppose we have

$$a^n x + b^n y = c^n, \tag{3.1}$$

and take x=y, so that

$$x = \frac{c^n}{a^n + b^n}. \tag{3.2}$$

Obviously, if $x \neq 1$ when n>2, then the theorem would be true, as has been proved [8]. Consider n=3, and

$$x = \frac{3^3}{1^3 + 2^3} = 3. \tag{3.3}$$

This would conform to Set 4 of Table 1 and the (*x*,*y*) class couple of $(\bar{3}_4, \bar{3}_4)$. For $x=y'$, we need $(\bar{1}_4, \bar{1}_4, r_1, r_1' = 0)$. From Table 1, the constraint for both *x* and *y* to be odd, excludes Sets 2,3, and 6. Thus only Sets 1,4, and 5 need to be considered. (Actually 1 and 4 will give the same results.) Table 6 shows what can be expected when *n* is even.

Set	c^n	a^n	b^n	x
1,4	$\bar{1}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$
5	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{2}_4$ or $\bar{0}_4$

Table 6: *n*> 2 and even

Note that

$$(4r_2 + 2)^n = 4(f(r_2)) \in \bar{0}_4$$

and

$$(4r_3 + 3)^n = (4(f(r_3) + 1)) \in \bar{1}_4, \text{ (}n\text{ even).}$$

When *n* is even, only Set 1 (or 4) needs to be considered.
An example is

$$c^4 = 17^4(\bar{1}_4), a^4 = 2^4(\bar{0}_4), b^4 = 1^4(\bar{1}_4)$$

which gives

$$x = 4913 = 17^3(\bar{1}_4).$$

The picture is more complex when *n* is odd (Table 7).

Type	Set	c^n	a^n	b^n	$(a+b)$	x
A	1,4	$\bar{1}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{1}_4$
B				$\bar{3}_4$	$\bar{3}_4$	$\bar{3}_4$
C		$\bar{3}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{3}_4$
D				$\bar{3}_4$	$\bar{3}_4$	$\bar{1}_4$
E	5	$\bar{0}_4$	$\bar{1}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{2}_4, \bar{0}_4$
F			$\bar{1}_4$	$\bar{3}_4$	$\bar{0}_4$	$\bar{0}_4, \bar{1}_4, \bar{2}_4, \bar{3}_4$
G			$\bar{3}_4$	$\bar{3}_4$	$\bar{2}_4$	$\bar{2}_4, \bar{0}_4$

Table 7: *n* odd

Some examples for $x \in \bar{1}_4$ (Types A, D and F) are given in Table 8 with *n*=3; (*x* must be in $\bar{1}_4$ when *x*=1).

When *c* is a prime, *p*, and *n*=3, $(a^3 + b^3) = p^2$ or *p* for integer *x*. However since,

$$(a^3 + b^3) = (a + b)(a^2 - ab + b^2) \tag{3.4}$$
$$\neq p$$

unlike $\left(a^4+b^4\right)$ which can be a prime. If

$$\left(a^3+b^3\right)=p^2$$

and

$$(a+b)=\left(a^2-ab+b^2\right)$$

then this only occurs for p=3 when a=2 and b=1 or *vice versa.* If

$$(a+b)=p^2,$$

then

$$(a+b)^2-3ab\neq p$$

or *vice versa* and hence $x\neq 1$.
Similar results occur for $c=p_1p_2\ldots$. In general, with $N=a+b$,

$$a^3+b^3=N\left(3a^2-3aN+N^2\right).$$

Type	c	a	b	x	Class of x
A	9	1	2	$81\left(3\times 3^3\right)$	$\bar{1}_4$
$c^n\in\bar{1}_4$	21	1	2	$1029\times\left(3\times 7^3\right)$	$\bar{1}_4$
$a^n\in\bar{0}_4$	33	1	2	$3993\times\left(3\times 11^3\right)$	$\bar{1}_4$
$b^n\in\bar{1}_4$	65	1	4	$4225\times(13\times 5)$	$\bar{1}_4$
D	27	6	3	$81\times\left(3^4\right)$	$\bar{1}_4$
$c^n\in\bar{3}_4$	35	2	3	$1225\times\left(35^2\right)$	$\bar{1}_4$
$a^n\in\bar{0}_4$	$3\times 5\times 13$	12	3	$4225\times\left(5\times 13^2\right)$	$\bar{1}_4$
$b^n\in\bar{3}_4$	$3\times 15\times 19$	8	7	$27075\times\left(5\times 15\times 19^2\right)$	$\bar{1}_4$
F	$2^m\times 7$	1	3	$2^{3m-2}\times 7^2$	$\begin{cases}\bar{2}_4, & m=1\\ \bar{0}_4, & m>1\end{cases}$
$c^n\in\bar{0}_4$	$2^m\times 19$	5	3	$2^{3m-3}\times 19^2$	$\begin{cases}\bar{1}_4, & m=1\\ \bar{0}_4, & m>1\end{cases}$
$a^n\in 1_4$					
$b^n\in\bar{3}_4$					

Table 8: Types A, D and F for $x\in\bar{1}_4$

Fermat's consideration of Equation (3.1) would probably have persuaded him that a value of unity for x was impossible to achieve generally. It should be noted that Fermat proved his theorem for n=3 and 4 via the method of infinite descent (inapplicable to the general case) before his famous marginal notation, so that Diophantus might well have inspired the more general proof that he claimed.

As Fermat must have found, when n is odd a^n+b^n always yields at least two prime factors. For Set A, then

$$a^n + b^n = \left(\bar{1}_4\right)^i \left(\bar{3}_4\right)^j. \tag{3.5}$$

That is, there will be *i* factors in $\bar{1}_4$ and *j* factors in $\bar{3}_4$, but since $a^n + b^n \in \bar{1}_4$, *j* must always be even (including *j*=0) because $\left(\bar{3}_4\right)^2 \in \bar{1}_4$ but $\left(\bar{3}_4\right)^3 \in \bar{3}_4$ and $\left(\bar{1}_4\right)^n \in \bar{1}_4$. Hence, the factors of $a^n + b^n \notin \bar{3}_4$ for an *x*=1 solution.

$a \in \bar{2}_4$	$b \in \bar{1}_4$	Class factors of $a^n + b^n$	
		n=3	*n*=5
2	1	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4$
2	5	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$
2	9	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{1}_4\ \bar{3}_4$
2	13	$\bar{1}_4\ \bar{3}_4\ \bar{3}_4$	$\bar{1}_4\ \bar{1}_4\ \bar{3}_4\ \bar{3}_4$
2	17	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{3}_4$
2	21	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{1}_4\ \bar{1}_4\ \bar{3}_4$
6	1	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$
6	5	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4$
6	21	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4$
6	25	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4\ \bar{1}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$
6	29	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{1}_4\ \bar{1}_4\ \bar{3}_4\ \bar{3}_4$
10	5	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4\ \bar{1}_4\ \bar{1}_4$	$\bar{1}_4\ \bar{1}_4\ \bar{1}_4\ \bar{1}_4\ \bar{1}_4\ \bar{3}_4\ \bar{3}_4$
10	9	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$
10	13	$\bar{3}_4\ \bar{3}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$
10	17	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{1}_4\ \bar{3}_4$
14	13	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{3}_4\ \bar{1}_4$
18	17	$\bar{3}_4\ \bar{3}_4\ \bar{1}_4$	$\bar{1}_4\ \bar{1}_4\ \bar{3}_4\ \bar{3}_4$

Table 9: Occurrence of $\bar{3}_4$ type factors

When $a \in \bar{2}_4, \bar{3}_4$ type factors always occur (Table 9), but when $a \in \bar{0}_4, \bar{1}_4$ type factors can occur without any $\bar{3}_4$ factors (Table 10). Thus for confirmation that *x*=1 never occurs we need only consider the factors of

$$\left((4r_0)^n + (4r_1 + 1)^n\right).$$

For *x*=1, we need $(4r_1 + 1)^n$ when $c = 4r_1 + 1$. However, $\left(4r_1^{/} + 1\right)^m \left(4r_1^{//} + 1\right)$ will only be found (Table 10) and this class type will occur around 30% of the factor structure, the remainder has $\bar{3}_4$ factors. When $a \in \bar{2}_4, a = 4r_2 + 2, b = 4r_1 + 1$, then

$$\left(a^3 + b^3\right) = 4^3\left(r_1^3 + r_2^3\right) + 48\left(r_1^2 + 2r_2^2\right) + 12\left(r_1 + 4r_2\right) + 9. \tag{3.6}$$

From Table 9 it can be seen that that $\left(a^3+b^3\right)=\bar{3}_4\bar{3}_4$ will cover all cases since $\bar{1}_4\times\bar{3}_4=\bar{3}_4$. Thus

$$a^3+b^3=\left(4r_3+3\right)\left(4r_3^{/}+3\right). \tag{3.7}$$

Comparing Equations (3.6) and (3.7) we get

$$16\left(r_1^3+r_2^3\right)+12\left(r_1^2+2r_2^2\right)+3(r_1+4r_2)=4r_3r_3^{/}+3\left(r_3+r_3^{/}\right). \tag{3.8}$$

Various combinations from the left hand side of Equation (3.8) may be equated to the terms on the right hand side (Table 11). Solutions for $\left(r_3,r_3^{/}\right)$ can thus be found.

$a\in\bar{0}_4$	$b\in\bar{1}_4$	Class factors of a^n+b^n	
		n=3	n=5
4	1	$\bar{1}_4\,\bar{1}_4$	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4$
4	5	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{1}_4$
4	9	$\bar{1}_4\,\bar{1}_4$	$\bar{1}_4\,\bar{1}_4$
4	13	$\bar{3}_4\,\bar{1}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{1}_4\,\bar{1}_4$
4	17	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4$
4	21	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4$	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4\,\bar{3}_4\,\bar{3}_4$
4	25	$\bar{1}_4\,\bar{1}_4$	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4$
4	29	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{1}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4$
8	9	$\bar{3}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{1}_4\,\bar{3}_4$
8	17	$\bar{1}_4\,\bar{1}_4\,\bar{3}_4\,\bar{3}_4$	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4\,\bar{1}_4$
12	13	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4$	$\bar{1}_4\,\bar{1}_4\,\bar{1}_4\,\bar{3}_4\,\bar{3}_4\,\bar{1}_4$
12	21	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{1}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{1}_4$
16	5	$\bar{3}_4\,\bar{3}_4\,\bar{3}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{3}_4\,\bar{1}_4\,\bar{1}_4$
16	13	$\bar{3}_4\,\bar{1}_4\,\bar{3}_4$	$\bar{3}_4\,\bar{1}_4\,\bar{3}_4$

Table 10: Occurrence of $\bar{1}_4$ type factors

Code	Equivalences	
A	$r_3+r_3^{/}$	$4r_3r_3^{/}$
	$4\left(r_1^2+2r_2^2\right)$	$16\left(r_1^3+r_2^3\right)+3\left(r_1+4r_2\right)$
B	$4\left(r_1^2+r_2\right)+r_1$	$16\left(r_1^3+r_2^3\right)+24r_2^2$
C	$4r_1^2+r_1$	$16\left(r_1^3+r_2^3\right)+24r_2^2+12r_2$

Table 11: Equivalences for Equation (3.8)

With $a = 4r_0 \in \bar{0}_4, b = (4r_1 + 1) \in \bar{1}_4$ some factor clusters arise without the $\bar{3}_4$ class. However, $(\bar{1}_4)^n$ factors (n odd) do not occur without other factors, either $\bar{1}_4$ or $(\bar{3}_4)^m$ (m even). For this case:

$$a^3 + b^3 = 4^3(r_0^3 + r_1^3) + 48r_1^2 + 12r_1 + 1 \tag{3.9}$$

and

$$a^3 + b^3 = (4r_1' + 1)(4r_1'' + 1), \tag{3.10}$$

since the factors of $(a^n + b^n)$ may be reduced to two as $(\bar{3}_4)^n \in \bar{1}_4$ (n even) and $(\bar{1}_4)^n \in \bar{1}_4$ (n odd or even) as pointed previously. On comparing Equations (3.9) and (3.10) we find

$$16(r_0^3 + r_1^3) + 12r_1^2 + 3r_1 = 4r_1'r_1'' + (r_1' + r_1''). \tag{3.11}$$

As with $a \in \bar{2}_4$ above, various combinations from the left hand side of Equation (3.11) may be equated to the two terms on the right hand side. For example, two such combinations are:

$$r_1' + r_1'' = 2(r_0^3 + r_1^3);$$
$$4r_1'r_1'' = 14(r_0^3 + r_1^3) + 12r_1^2 + 3r_1,$$

and

$$r_1' + r_1'' = 4r_1^2 - 1;$$
$$4r_1'r_1'' = 16(r_0^3 + r_1^3) + 8r_1^2 + 1.$$

Equation (3.2) may be re-written as

$$x = \frac{c^n}{a^n + b^n} = \frac{(\frac{c}{b})^n}{1 + (\frac{a}{b})^n},\ a < b. \tag{3.12}$$

When n is large, $(a/b)^n$ is very small, so that the denominator reduces to 1, and if x=1, then c=b which is not acceptable; so for large n, $x \neq 1$. If (a/b) =0.5, then $(a/b)^{20} \approx 10^{-6}$, or if ($a$/$b$)=0.9, then $(a/b)^{150} \approx 10^{-7}$.

Similar analyses to the above may be made for D and F (n odd), and for Sets 1 and 4 when n is even. Aurifeuillian Factorizations [7] could be useful in the latter case. For instance,

$$a^6 + b^6 = (a^2 + b^2)((a^2 + 3ab + b^2)^2 - 6ab(a + b)^2); \tag{3.13}$$

with a=2, b=3, the factors are 13 and 61. It is of interest that when a or $b \in \bar{3}_4$, $(a^4 + b^4)$ produces a large number of primes. This too can be explained by the underlying integer structure.

4. Final Comments

It should be noted that a linear congruence $ax \equiv c \pmod{b}$ (where a and c are known residue classes and x an unknown residue class which satisfies the linear congruence) is equivalent to the Diophantine equation

$$ax - by = c. \tag{4.1}$$

It is of interest to note that the Chinese Remainder Theorem [7] covers a system of simultaneous such congruences. Clarke [2] has also used modular arithmetic to classify solutions of such equations. Elsewhere [1] he has applied his ideas to the building industry. Yates [9] has combined modular arithmetic with repunits to study primality. The aim of this paper though has been to provide an alternative approach to solving Diophantine equations.

When the parity of either *x* or *y* is constrained the solution is much simpler. However, the more complex systems 5 and 6 in Table 1 are interesting since they show the underlying order of the integers interacting with each other.

Modular rings such as Z_6 or Z_8 [4,6] may be used in a similar manner: for example, in Z_6, in which an integer *N* is represented by $6r_i + (\bar{i} - 3)$. $\bar{3}_6, \bar{6}_6 \subset Z_6$ have $3|N$, while $\bar{2}_6$ and $\bar{4}_6$ contain all the primes. $\bar{2}_6$ and $\bar{5}_6$ contain no even powers [4]. When Z_6 is used for Set 5, the permissible (*x*,*y*) class couples are

$$(\bar{6}_6, \bar{4}_6), (\bar{3}_6, \bar{3}_6), (\bar{6}_6, \bar{2}_6), (\bar{3}_6, \bar{1}_6), (\bar{6}_6, \bar{6}_6), (\bar{3}_6, \bar{5}_6),$$

which, with $c \in \bar{3}_6$, yield the (*x*,*y*) couples of Table 5 in the same order.

An interesting assumption is that the generalized "Last Theorem" of Fermat may well have derived from his study of the Diophantine Equations. The factor structure of the sum of two powers prevents the sum from equalling an integer of the same power.

References

1. J.H. Clarke, Linear Diophantine Equations Applied to Modular Co-ordination, *Australian Journal of Applied Science*, **15(4)** (1964): 201-4.
2. J.H. Clarke, Conditions for the Solution of a Linear Diophantine Equation, *New Zealand Mathematics Magazine*, **14(1)** (1977): 45-47.
3. J. Hunter, *Number Theory*. Edinburgh: Oliver and Boyd, 1964.
4. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, Integer Class Properties Associated with an Integer Matrix. *Notes on Number Theory & Discrete Mathematics*. **1 (2)** (1995): 53-59.
5. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, Analysis of Diophantine Properties Using Modular Rings with Four and Six Classes. *Notes on Number Theory & Discrete Mathematics*. **3 (2)** (1997): 61-74.
6. J.V. Leyendekkers & A.G. Shannon, Analyses of Row Expansions within the Octic 'Chess' Modular Ring, Z_8. *Notes on Number Theory & Discrete Mathematics*. **5(3)** (1999): 102-114.
7. Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. 2nd edition. Progress in Mathematics, Volume 126. Boston: Birkhäuser, 1994.
8. A.J. van der Poorten, *Notes on Fermat's Last Theorem*. New York: Wiley.
9. S. Yates, The Mystique of Repunits, *Mathematics Magazine*, **51(1)**: (1978): 22-28.

AMS Classification Numbers: 11A41, 11A07