NNTDM 4 (1998) 1, 1-17

THE CHARACTERISTICS OF PRIMES AND OTHER INTEGERS WITHIN THE MODULAR RING $\mathbb{Z}_4$ AND IN CLASS $\overline{1}$

J.V. Leyendekkers and J.M. Rybak
The University of Sydney, 2006, Australia
A.G. Shannon
University of Technology, Sydney, 2007, Australia

ABSTRACT

The integer structure of Class $\overline{1}$ in the modular ring $\mathbb{Z}_4$ has been analysed in detail. Most integers of this category equal a sum of two squares $(x^2 + y^2)$. Those that do not are non-primes. The primes are distinguished by having a unique $< x, y >$ pair that has no common factors. Other integers in Class $\overline{1}$ have multiple values of $< x, y >$ or more rarely a single $< x, y >$ pair with common factors. Methods of estimating $< x, y >$ pairs are given. These are based on the class structure within $\mathbb{Z}_4$ and the right-most end digit characteristics. The identification of primes is consequently facilitated.

1. INTRODUCTION

The modular ring $\mathbb{Z}_4$ has been described in detail elsewhere [1]. Briefly, each integer, n, within this ring satisfies the relationship

$$n = 4r_i + i \tag{1.1}$$

where i is the class, $\overline{0}, \overline{1}, \overline{2}$ or $\overline{3}$ and r is the row within the class; classes $\overline{1}$ and $\overline{3}$ contain the odd numbers.

Primes, p, and non-primes, m, are easily sorted using the relationship deduced previously [2] to identify m, namely

$$m = (2(s + t) - 1)(2t + 1) \tag{1.2}$$

where s and $t = 1, 2, 3, \ldots, s = 0$ gives a square.

In the present paper we shall confine our analysis to class $\overline{1}$. This class has the distinction that it contains primes that follow:

$$p = x^2 + y^2 \tag{1.3}$$

where x is even and y odd. Class $\overline{3}$ contains no such primes, and integers in this class will be discussed in a later paper.

As noted previously [1] the largest component of a primitive Pythagorean triple equals the sum of squares and hence is confined to class $\overline{1}$ in $\mathbb{Z}_4$.

Not all integers in class $\overline{1}$ equal the sum of squares and such integers, which are non-primes, can only be one of the minor components of a Pythagorean triple. For example, 77 falls in class $\overline{1}$ and in row 19 and is not equal to a sum of squares; it appears as the second largest component in the triple $< 85, 77, 36 >$.

When n is a prime only one set of x, y occurs. If n equals a sum of squares and x and y can have more than one value, then n must be a non-prime. However, a few non-primes have unique x, y values or none at all so that it is important to characterise the integers precisely so that a given number n can be identified as a prime or not. We shall first examine the non-primes in some detail.

2. NON-PRIMES IN CLASS $\overline{1}$

The class of a non-prime odd number, m, will depend on the classes of s and t (equation 1.2). If s and t are both even, m falls in class $\overline{3}$. If s falls in class $\overline{0}$, the row is odd, whereas s in class $\overline{2}$ finds m in an even row. When t is odd, the parity of the rows reverse.

When s is odd, m falls in class $\overline{1}$. With s in class $\overline{1}$, the rows are all even, but if s falls in class $\overline{3}$, the rows are all odd (Table 2.1).

Since x is even and y odd, the $< x, y >$ class pairs $< \overline{2}, \overline{1} >$, $< \overline{2}, \overline{3} >$ and $< \overline{0}, \overline{1} >$, $< \overline{0}, \overline{3} >$ need to be considered. The first two pairs give an odd row for m so that we shall consider these first.

		CLASS of m		
t	s $\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{3}$	$\overline{1}$
$\overline{1}$	$\overline{3}$	$\overline{1}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{1}$	$\overline{3}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{3}$	$\overline{1}$
	t even, rows odd, t odd, rows even	rows all even	t even, rows even, t odd, rows odd	rows all odd

TABLE 2.1: Non-prime integer distribution

2.1 Odd rows for m in class $\overline{1}$.

Tables 2.2 and 2.3 show an array of numbers in the $< x, y >$ class pairs of $< \overline{2}, \overline{1} >$ and $< \overline{2}, \overline{3} >$. The bracketed values are primes. All integers that are perfect squares or have a factor of 5 or 3 are easily distinguished from primes so that only the other values of m are considered.

It is found that all except five of these latter integers, which equal the sum of squares can be accommodated in the $< s, t >$ class pairs of $< \overline{3}, \overline{0} >$ or $< \overline{3}, \overline{2} >$. For the $< \overline{3}, \overline{0} >$ pair, $s = 4r_3 + 3$ and $t = 4r_0$ so that equation (1.2) becomes

$$m = (8(r_3 + r_0) + 5)(8r_0 + 1) \tag{2.1}$$

In this case factors for m will include $17, 41, 49, 61, \ldots$ whilst for the $< \overline{3}, \overline{2} >$ set, $s = 4r_3 + 3$ and $t = 4r_2 + 2$, so that

$$m = (8(r_3 + r_2) + 9)(8r_2 + 5) \tag{2.2}$$

and factors will include $13, 29, 37, 53, \ldots$.

r_1 \ r_2	0	1	2	3	4	5	6	7	8	9	10
0	(5)	(37)	(101)	(197)	325	485	(677)	901	1157	1445	1765
1	(29)	(61)	125	221	(349)	(509)	(701)	925	(1181)	1469	(1789)
2	85	117	(181)	(277)	405	565	(757)	981	(1237)	1525	1845
3	(173)	205	(269)	365	493	(653)	845	(1069)	1325	(1613)	(1933)
4	(293)	325	(389)	485	(613)	(773)	965	1189	1445	(1733)	(2053)
5	445	477	(541)	637	765	925	(1117)	1341	(1597)	1885	2205
6	629	(661)	725	(821)	949	(1109)	(1301)	1525	1781	(2069)	(2389)
7	845	(877)	(941)	1037	1165	1325	1517	(1741)	(1997)	2285	2605
8	(1093)	1125	1189	1285	1413	1573	1765	1989	2245	2533	2853
9	(1373)	1405	1469	1565	(1693)	1853	2045	(2269)	2525	2813	3133
10	1685	1717	1781	(1877)	2005	2165	(2357)	2581	(2837)	3125	3445

TABLE 2.2: $< x, y >$ Class pair $< \overline{2}, \overline{1} >$

m values prime to 3 and 5 and not perfect squares have been taken from Tables (2.2) and (2.3) and are listed in Table 2.4 (the $< s, t >$ class pair $< \overline{3}, \overline{0} >$) or in Table 2.5 (the $< s, t >$ class pair $< \overline{3}, \overline{2} >$). We have taken the smallest of the two factors (a prime) as $(2t + 1)$, that is $(8r_0 + 1)$ or $(8r_2 + 5)$.

As can be seen, all values of m have two values of $< x, y >$. This distinguishes them from the primes which have unique values for $< x, y >$.

r_3 \ r_2	0	1	2	3	4	5	6	7	8	9	10
0	(13)	45	(109)	205	333	493	685	909	1165	(1453)	1773
1	(53)	85	(149)	245	(373)	533	725	949	1205	(1493)	1813
2	125	(157)	221	(317)	445	605	(797)	(1021)	(1277)	1565	1885
3	(229)	261	325	(421)	549	(709)	901	1125	(1381)	(1669)	1989
4	365	(397)	(461)	(557)	685	845	1037	1261	1517	1805	2125
5	533	565	629	725	(853)	(1013)	1205	(1429)	1685	(1973)	(2293)
6	(733)	765	(829)	925	1053	(1213)	1405	1629	1885	2173	2493
7	965	(997)	(1061)	1157	1285	1445	(1637)	(1861)	2117	2405	2725
8	(1229)	1261	1325	1421	(1549)	(1709)	(1901)	2125	(2381)	2669	2989
9	1525	1557	(1621)	1717	1845	2005	2197	2421	(2677)	2965	3285
10	1853	1885	(1949)	2045	2173	(2333)	2525	(2749)	3005	3293	(3613)

TABLE 2.3: $< x, y >$ class pair $< \overline{2},\overline{3} >$

m	Factors	r_3	r_0	s	t	x	y	$\langle x, y \rangle$ Class
493	29×17	1	2	7	8	18	13	$\langle \overline{2},\overline{1} \rangle$
						22	3	$\langle \overline{2},\overline{3} \rangle$
629	37×17	2	2	11	8	2	25	$\langle \overline{2},\overline{1} \rangle$
						10	23	$\langle \overline{2},\overline{3} \rangle$
901	53×17	4	2	19	8	30	1	$\langle \overline{2},\overline{1} \rangle$
						26	15	$\langle \overline{2},\overline{3} \rangle$
1037	61×17	5	2	23	8	26	19	$\langle \overline{2},\overline{3} \rangle$
						14	29	$\langle \overline{2},\overline{1} \rangle$
1717	101×17	10	2	43	8	6	41	$\langle \overline{2},\overline{1} \rangle$
						14	39	$\langle \overline{2},\overline{3} \rangle$
1853	109×17	11	2	47	8	2	43	$\langle \overline{2},\overline{3} \rangle$
						22	37	$\langle \overline{2},\overline{1} \rangle$
2173	53×41	1	5	7	20	38	27	$\langle \overline{2},\overline{3} \rangle$
						18	43	$\langle \overline{2},\overline{3} \rangle$
2533	149×17	16	2	67	8	38	33	$\langle \overline{2},\overline{1} \rangle$
						18	47	$\langle \overline{2},\overline{3} \rangle$
2669	157×17	17	2	71	8	38	35	$\langle \overline{2},\overline{3} \rangle$
						50	13	$\langle \overline{2},\overline{1} \rangle$

TABLE 2.4: $< s, t >$ class pair $< 3, 0 >$ (equation 2.1)

m	Factors	r_3	r_2	s	t	x	y	$\langle x,y\rangle$ Class
221	17×13	0	1	3	6	14	5	$\langle\overline{2},\overline{1}\rangle$
						10	11	$\langle\overline{2},\overline{3}\rangle$
533	41×13	3	1	15	6	22	7	$\langle\overline{2},\overline{3}\rangle$
						2	23	$\langle\overline{2},\overline{3}\rangle$
949	73×13	7	1	31	6	18	25	$\langle\overline{2},\overline{1}\rangle$
						30	7	$\langle\overline{2},\overline{3}\rangle$
1157	89 x 13	9	1	39	6	34	1	$\langle\overline{2},\overline{1}\rangle$
						14	31	$\langle\overline{2},\overline{3}\rangle$
1189	41×29	1	3	7	14	10	33	$\langle\overline{2},\overline{1}\rangle$
						30	17	$\langle\overline{2},\overline{1}\rangle$
1261	97×13	10	1	43	6	30	19	$\langle\overline{2},\overline{3}\rangle$
						6	35	$\langle\overline{2},\overline{3}\rangle$
1469	113×13	12	1	51	6	10	37	$\langle\overline{2},\overline{1}\rangle$
						38	5	$\langle\overline{2},\overline{1}\rangle$
1517	41×37	0	4	3	18	26	29	$\langle\overline{2},\overline{1}\rangle$
						34	19	$\langle\overline{2},\overline{3}\rangle$
1781	137×13	15	1	63	6	10	41	$\langle\overline{2},\overline{1}\rangle$
						34	25	$\langle\overline{2},\overline{1}\rangle$
2117	73×29	5	3	23	14	34	31	$\langle\overline{2},\overline{3}\rangle$
						46	1	$\langle\overline{2},\overline{1}\rangle$
2197	169×13	19	1	79	6	26	39	$\langle\overline{2},\overline{3}\rangle$
						46	9	$\langle\overline{2},\overline{1}\rangle$
2581	89×29	7	3	31	14	30	41	$\langle\overline{2},\overline{1}\rangle$
						50	9	$\langle\overline{2},\overline{1}\rangle$
2813	97×29	8	3	35	14	2	53	$\langle\overline{2},\overline{1}\rangle$
						38	37	$\langle\overline{2},\overline{1}\rangle$
3133	241×13	28	1	115	6	42	37	$\langle\overline{2},\overline{1}\rangle$
						18	53	$\langle\overline{2},\overline{1}\rangle$
3293	89×37	6	4	27	18	22	53	$\langle\overline{2},\overline{1}\rangle$
						38	43	$\langle\overline{2},\overline{3}\rangle$

TABLE 2.5: $< s,t >$ class pair $< \overline{3},\overline{2} >$ (equation 2.2)

The five remaining non-primes, 637, 1421, 1573, 1813 and 2989 fall in either

$$< s,t > \;=\; < \overline{3},\overline{1} >$$

or $$< s,t > \;=\; < \overline{3},\overline{3} > .$$

For the $< \overline{3},\overline{1} >$ class pair $m = (8(r_3 + r_1) + 7)(8r_1 + 3)$ (2.3)
which gives the lowest factor for m of $11, 19, 43, \ldots$.

For the $< \overline{3},\overline{3} >$ class pair

$$m = (8(r_3 + r_3{}') + 11)(8r_3 + 7) \tag{2.4}$$

which gives the lowest factors for m as $7, 23, 31, \ldots$.

The characteristics of these integers are given in Table 2.6

$< x,y >$ class pair $< \overline{2},\overline{k} >$	$< s,t >$ class pair $< \overline{i},\overline{j} >$	m	Factors	r_i	r_j	r_2	r_k	s	t
$\overline{2},\overline{1}$	$\overline{3},\overline{1}$	1573	143×11	16	1	5	8	67	5
	$\overline{3},\overline{3}$	637	91×7	10	0	3	5	43	3
$\overline{2},\overline{3}$	$\overline{3},\overline{1}$	nil							
	$\overline{3},\overline{3}$	1421	203×7	24	0	3	8	99	3
		1813	259×7	31	0	10	1	127	3
		2989	427×7	52	0	10	8	211	3

TABLE 2.6: Characteristics of integers

Other values of m for these two $< s,t >$ class pairs $< \overline{3},\overline{3} >$ and $< \overline{3},\overline{1} >$ are given in Table 2.7. Like the integers in Table 2.6, a few of the integers in Table 2.7 which are underlined (45, 117 and 1053) equal a sum of squares with unique values for x and y. However, they are divisible by 3 as are the m values. The other integers in Table 2.7 are not equal to a sum of squares and these could never be the major component in a primitive Pythagorean triple.

r_1	m						r_3'	m					
r_3	0	1	2	3	4	5		r_3	0	1	2	3	4	5
0	21	<u>45</u>	69	93	<u>117</u>	141	0		77	285	621	1085	1677	2397
1	165	253	341	429	517	605	1		133	405	805	1333	1989	2773
2	437	589	741	893	1045	1197	2		189	525	989	1581	2301	3149
3	837	<u>1053</u>	1269	1485	1701	1917	3		245	645	1173	1829	2613	3525
4	1365	1645	1925	2205	2485	2765	4		301	765	1357	2077	2925	3901
5	2021	2365	2709	3053	3397	3741	5		357	885	1541	2325	3237	4277

(a) $< s,t > \;=\; < \overline{3},\overline{1} >$ (equation 2.3) (b) $< s,t > \;=\; < 3,3 >$ (equation 2.4)

TABLE 2.7

3. PRIMES IN CLASS $\overline{1}$ AND IN ODD ROWS

The above m functions have the general form

$$m = \big(8(r_i + r_j) + (g+4)\big)(8r_i + g) \tag{3.1}$$

where $g = 1, 3, 5$ or 7.

Equation (3.1) expands to

$$m = 64r_i(r_i + r_j) + 16(g+2)r_i + 8gr_j + g(g+4) \tag{3.2}$$

and since $g(g+4) = 5 + 8h$, with $h = 0, 2, 5$ or 9,

$$m = 8R_3{}' + 5 \tag{3.3}$$

where $R_3{}' = (8r_i(r_i + r_j) + 2(g+2)r_i + gr_j + h)$. (3.4)

If m reduces to a prime, the term $(8r_i + g)$ from equation (3.1) would equal unity; that is $r_i = (1-g)/8$, so that r_i equals zero or a negative fraction.

Substitution into equation (3.4) shows that

$$R_3{}' = r_j \tag{3.5}$$

since $(5 - g^2 - 4g)/8 + h = 0$. Hence

$$p = 4(2R_3{}' + 1) + 1 \tag{3.6}$$

which is consistent with p being in class $\overline{1}$, in an odd row. For the $< x, y >$ set in $< \overline{2}, \overline{1} >$, that is with $y = 4R_1 + 1$, it is found that $R_3{}'$ and R_1 occupy the same relative classes. The same applies for the $< x, y >$ class pair in $< \overline{2}, \overline{3} >$ (Table 3.1). Consequently, y follows the function

$$y = 16\overline{r}_i + q \tag{3.7}$$

where $\overline{r}_i$ is the row for R_1 or R_3, q values are listed in Table 3.1.

In order to make the function for y more specific, consider the right-most digit (RMD) of the integers and use the fact that even squares must end in $0, 4$ or 6 whilst odd squares end in $1, 5$ or 9.

	$< x, y > = < \overline{2}, \overline{1} >$		$< x, y > = < \overline{2}, \overline{3} >$	
R_3'	R_1	q_1	R_3	q_3
$\overline{0}$	$\overline{0}$	1	$\overline{3}$	15
$\overline{2}$	$\overline{2}$	9	$\overline{1}$	7
$\overline{3}$	$\overline{1}$	5	$\overline{2}$	11
$\overline{1}$	$\overline{3}$	13	$\overline{0}$	3

TABLE 3.1: Class Structures

An asterisk indicates that the right-most digit of the quantity is being considered (Table 3.2). We have included $n* = 5$, but since integers not prime to 5 (except 5) are distinct from odd primes they will not feature in our present analysis.
If $y* = 1$ then $y = 1, 11, 21, 31, \ldots$. However, if y is in class $\overline{1}$, only the values $1, 21, 41\ldots$, apply; whilst if y *is* in class $\overline{3}$, the values $11, 31, 51, \ldots$ apply. Hence, in general.

$$y = y_0 + 20\bar{t}. \tag{3.8}$$

Equating equations (3.7) and (3.8) we obtain

$$\bar{t} = (4\overline{r}_i + (q - y_0)/4)/5 \tag{3.9}$$

which, with the above data, reduces to

$$\bar{t} = \bar{t}_0 + 8\overline{s}, \tag{3.10}$$

so that

$$y = (y_0 + 20\bar{t}_0) + 160\overline{s}. \tag{3.11}$$

Values of y_0 and $\bar{t}_0$ for the different $\overline{r}_i$ are given in Tables 3.3 and 3.4. Maximum y will, of course, be $(n-4)^{\frac{1}{2}}$.

n^*	x^{2^*}	x^*	y^{2^*}	y^*
1	0	0	1	9,1
	6	4,6	5	5
3	4	2,8	9	7,3
5	0	0	5	5
	4	2,8	1	1,9
	6	4,6	9	7,3
7	6	4,6	1	1,9
9	0	0	9	7,3
	4	2,8	5	5

TABLE 3.2: Development of Equation (3.7)

$y*$	y_0	$\overline{r}_0*$	$\bar{t}_{00}$	$\overline{r}_2*$	$\bar{t}_{02}$	$\overline{r}_1*$	$\bar{t}_{01}$	$\overline{r}_3*$	$\bar{t}_{03}$
1	11	8,3	6,2	0,5	0,4	4,9	3,7	6,1	5,1
9	19	6,1	4,0	8,3	6,2	2,7	1,5	4,9	3,7
5	15	2,7	1,5	4,9	3,7	8,3	6,2	0,5	0,4
7	7	4,9	3,7	6,1	5,1	0,5	0,4	2,7	2,6
3	3	0,5	0,4	2,7	2,6	6,1	5,1	8,3	7,3

TABLE 3.3: Class couple $< x, y > = < \overline{2}, \overline{3} >$

$y*$	y_0	$\overline{r}_0*$	$\overline{t}_{00}$	$\overline{r}_2*$	$\overline{t}_{02}$	$\overline{r}_1*$	$\overline{t}_{01}$	$\overline{r}_3*$	$\overline{t}_{03}$
1	1	0,5	0,4	2,7	2,6	6,1	5,1	8,3	7,3
9	9	8,3	6,2	0,5	0,4	4,9	3,7	6,1	5,1
5	5	4,9	3,7	6,1	5,1	0,5	0,4	2,7	2,6
7	17	6,1	4,0	8,3	6,2	2,7	1,5	4,9	3,7
3	13	2,7	1,5	4,9	3,7	8,3	6,2	0,5	0,4

TABLE 3.4: Class couple $< x, y > = < \overline{2}, \overline{1} >$

Examples of integer analysis using equation (3.11) and the above tables are summarised in Tables 3.5 to 3.7. The primes have a unique value for $< x, y >$, whereas the majority of non-primes either have multiple values, or none at all. The fifth listed integer is an example of the latter.

Such integers fall in $< s, t >$ class pairs $< \overline{3}, \overline{1} >$ or $< \overline{3}, \overline{3} >$. For class pair $< \overline{3}, \overline{1} >$ possible factors are obtained from $(8r_1 + 3)$. Discarding values not prime to 3 and 5 we get $11, 19, 43, 59, 67, 83, 91, 107, 131, \ldots$. The maximum must be less than $m^{\frac{1}{2}}$. For the class pair $< \overline{3}, \overline{3} >$ possible factors are obtained from $(8r_3 + 7)$, excluding those not prime to 3 or 5. This gives $23, 31, 47, 71, 79, 87, 103, 119, 127, \ldots$. The factors for 113053 are 863×131, so that combining the factors for class couples $< \overline{3}, \overline{1} >$ and $< \overline{3}, \overline{3} >$ in increasing numerical order we obtain eighteen possible factors. The results show that the required integer lies in the $< s, t >$ couple class of $< \overline{3}, \overline{1} >$ with $r_1 = 16$ and $r_3 = 91$ with $s = 367$ and $t = 65$. The integer 1421 has only one set of $< x, y >$ values, but it is not prime to 7, and thus it falls in $< s, t >$ class couple $< \overline{3}, \overline{3} >$, with factors 203×7 and $r_3 = 0, r_3{}' = 24$ and $< s, t > = < 99, 3 >$.

			CLASSES		
N_0	n	$R_3{}'$	$R_3{}'$	R_1	R_3
1	13949	1743	$\overline{3}$	$\overline{1}$	$\overline{2}$
2	107269	13408	$\overline{0}$	$\overline{0}$	$\overline{3}$
3	108277	13534	$\overline{2}$	$\overline{2}$	$\overline{1}$
4	3613	451	$\overline{3}$	$\overline{1}$	$\overline{2}$
5	113053	14131	$\overline{3}$	$\overline{1}$	$\overline{2}$
6	1421	177	$\overline{1}$	$\overline{3}$	$\overline{0}$

TABLE 3.5: Classes for Table 3.1

			$\langle x, y \rangle$ couple in $\langle \overline{2}, \overline{1} \rangle$				$\langle x, y \rangle$ couple in $\langle \overline{2}, \overline{3} \rangle$			
No	n^*	y^*	y_0	$\bar{t}_0$	$y_0 + 20\bar{t}_0$	max $\bar{s}$	y_0	$\bar{t}_0$	$y_0 + 20\bar{t}_0$	max $\bar{s}$
1	9	7	17	1,5	37,117	1,1	7	5,1	107,27	0,1
		3	13	6,2	133,53	1,1	3	2,6	43,123	0,1
		5	5	0,4	5,85	0,0	15	3,7	75,155	1,1
2	9	7	17	4,0	97,17	1,1	7	2,6	47,127	1,1
		3	13	1,5	33,113	1,1	3	7,3	143,63	1,1
		5	5	3,7	65,145	1,1	15	0,4	15,95	1,1
3	7	9	9	0,4	9,89	2,1	19	1,5	39,119	1,1
		1	1	2,6	41,121	1,0	11	3,7	71,151	1,1
4	3	7	17	1,5	37,117	0,0	7	5,1	107,27	0,0
		3	13	6,2	133,53	0,0	3	2,6	43,123	0,0
5	3	7	17	1,5	37,117	1,1	7	5,1	107,27	1,1
		3	13	6.2	133,53	1,1	3	2,6	43,123	1,1
6	1	9	9	5,1	109,29	0,0	19	4,0	99,19	0,0
		1	1	7,3	141,61	0,0	11	6,2	131,51	0,0
		5	5	2,6	45,125	0,0	15	1,5	35,115	0,0

TABLE 3.6: $y_0, \bar{t}_0$ from Tables 3.3 and 3.4

No	x	y	$< x, y >$ Class	Integer
			couple	
1	118	5	$< \overline{2}, \overline{1} >$	non-prime
	110	43	$< \overline{2}, \overline{3} >$	
	50	107	$< \overline{2}, \overline{3} >$	
	82	85	$< \overline{2}, \overline{1} >$	
2	238	225	$< \overline{2}, \overline{1} >$	prime
3	6	329	$< \overline{2}, \overline{1} >$	non-prime
	306	121	$< \overline{2}, \overline{1} >$	
4	42	43	$< \overline{2}, \overline{3} >$	prime
5	nil	nil	none	non-prime belongs in the $< s, t >$ class couple $< \overline{3}, \overline{1} >$, see text
6	14 (7×2)	35 (7×5)	$< \overline{2}, \overline{3} >$	non-prime belongs in the $< s, t >$ class couple $< \overline{3}, \overline{3} >$, see text

TABLE 3.7: $x = [n - y^2]^{\frac{1}{2}}$

4. EVEN ROWS FOR n IN CLASS $\overline{1}$

Equating $n = 4r_1 + 1$ to $x^2 + y^2$ with even class functions for x and odd class functions for y, we find that r_1 will be even when $< x, y > = < \overline{0}, \overline{1} >$ or $< \overline{0}, \overline{3} >$. Table 2.1 shows that the (s, t) class couples, when n is in an even row, are $< \overline{1}, \overline{0} >$, $< \overline{1}, \overline{1} >$, $< \overline{1}, \overline{2} >$ and $< \overline{1}, \overline{3} >$.

Tables 4.1 and 4.2 list integers for the $< x, y >$ class couples $< \overline{0}, \overline{1} >$ and $< \overline{0}, \overline{3} >$ respectively. The primes are bracketed and, as for the odd row case, we shall not concern ourselves with integers divisible by 5 or 3 or which are perfect squares. Tables 4.3 and 4.4 give a description of the non-primes. All have two or more values for the $< x, y >$ pair, and, for the integers considered, the $< s, t >$ class pair $< \overline{1}, \overline{2} >$ dominates.

Only two of the non-primes (2009 and 833, from $< x, y > = < \overline{0}, \overline{3} >$) fall in the $< s, t >$ class pair $< \overline{1}, \overline{3} >$; none fall in the $< s, t >$ class pair $< \overline{1}, \overline{1} >$.

Substituting in the class function for the $< s, t >$ couples, gives equation (1.2) as

$$m = (8(r_i + r_j) + g)(8r_i + g) \tag{4.1}$$

where $g = 1, 3, 5$ or 7 for $< \overline{j}, \overline{i} > = < \overline{1}, \overline{0} >$, $< \overline{1}, \overline{1} >$, $< \overline{1}, \overline{2} >$ and $< \overline{1}, \overline{3} >$, respectively.

Expanding equation (4.1) we find that

$$m = 64r_i(r_i + r_j) + 16gr_i + 8gr_j + g^2 \tag{4.2}$$

so that

$$m = 8R_1{}' + 1 \tag{4.3}$$

where

$$R_1{}' = (8r_i(r_i + r_j) + 2gr_i + gr_j + (g^2 - 1)/8 \tag{4.4}$$

When m reduces to a prime, then $r_i = (1 - g)/8$ as for the odd row case.

r_0 / r_1	0	1	2	3	4	5	6	7	8	9	10
0	1	(17)	65	145	(257)	(401)	(577)	785	1025	(1297)	(1601)
1	25	(41)	(89)	169	(281)	425	(601)	(809)	(1049)	(1321)	1625
2	81	(97)	145	225	(337)	481	657	865	1105	1377	1681
3	169	185	(233)	(313)	425	(569)	745	(953)	(1193)	1465	1769
4	289	305	(353)	(433)	545	689	865	1073	1313	1585	(1889)
5	441	(457)	505	585	697	841	1017	1225	1465	1737	2041
6	625	(641)	689	(769)	(881)	1025	(1201)	(1409)	1649	1921	2225
7	841	(857)	905	985	(1097)	1241	1417	1625	1865	(2137)	(2441)
8	1089	1105	(1153)	1233	1345	(1489)	1665	(1873)	(2113)	2385	(2689)
9	1369	1385	(1433)	1513	1625	1769	1945	(2153)	(2393)	2665	(2969)
10	1681	(1697)	1745	1825	1937	(2081)	2257	2465	2705	2977	3281

TABLE 4.1: $< x, y >$ class pair $< \overline{0}, \overline{1} >$

r_0 / r_3	0	1	2	3	4	5	6	7	8	9	10
0	9	25	(73)	153	265	(409)	585	793	(1033)	1305	(1609)
1	49	65	(113)	(193)	305	(449)	625	833	1073	1345	1649
2	121	(137)	185	265	377	(521)	697	905	1145	1417	(1721)
3	225	(241)	289	369	481	625	801	(1009)	(1249)	1521	1825
4	361	377	425	505	(617)	(761)	(937)	1145	1385	(1657)	1961
5	529	545	(593)	(673)	785	(929)	1105	1313	(1553)	1825	(2129)
6	729	745	793	873	985	(1129)	1305	1513	(1753)	2025	2329
7	961	(977)	1025	1105	(1217)	(1361)	1537	1745	1985	2257	2561
8	1225	1241	(1289)	1369	(1481)	1625	(1801)	2009	2249	(2521)	2825
9	1521	1537	1585	1665	(1777)	1921	2097	2305	2545	2817	(3121)
10	1849	1865	(1913)	(1993)	2105	2249	2425	(2633)	2873	3145	(3449)

TABLE 4.2: $< x, y >$ class pair $< \overline{0}, \overline{3} >$

m	Factors	r_1	r_2	s	t	x	y	$\langle x,y\rangle$ class pair
377	29×13	2	1	9	6	16	11	$\langle\overline{0},\overline{3}\rangle$
						4	19	$\langle\overline{0},\overline{3}\rangle$
481	37×13	4	1	13	6	16	15	$\langle\overline{0},\overline{3}\rangle$
						20	9	$\langle\overline{0},\overline{1}\rangle$
689	53×13	5	1	21	6	20	17	$\langle\overline{0},\overline{1}\rangle$
						8	25	$\langle\overline{0},\overline{1}\rangle$
793	61×13	6	1	25	6	8	27	$\langle\overline{0},\overline{3}\rangle$
						28	3	$\langle\overline{0},\overline{3}\rangle$
1073	37×29	1	3	5	14	28	17	$\langle\overline{0},\overline{1}\rangle$
						32	7	$\langle\overline{0},\overline{3}\rangle$
1313	101×13	11	1	45	6	32	17	$\langle\overline{0},\overline{1}\rangle$
						28	23	$\langle\overline{0},\overline{3}\rangle$
1417	109×13	12	1	49	6	24	29	$\langle\overline{0},\overline{1}\rangle$
						36	11	$\langle\overline{0},\overline{3}\rangle$
1537	53×29	3	3	13	14	24	31	$\langle\overline{0},\overline{3}\rangle$
						4	39	$\langle\overline{0},\overline{3}\rangle$
1769	61×29	4	3	17	14	40	13	$\langle\overline{0},\overline{1}\rangle$
						20	37	$\langle\overline{0},\overline{1}\rangle$
1937	149×13	17	1	69	6	16	41	$\langle\overline{0},\overline{1}\rangle$
						44	1	$\langle\overline{0},\overline{1}\rangle$
1961	53×37	2	4	9	18	40	19	$\langle\overline{0},\overline{3}\rangle$
						44	5	$\langle\overline{0},\overline{1}\rangle$
2041	157×13	18	1	73	6	4	45	$\langle\overline{0},\overline{1}\rangle$
						40	21	$\langle\overline{0},\overline{1}\rangle$
2249	173×13	20	1	81	6	32	35	$\langle\overline{0},\overline{3}\rangle$
						20	43	$\langle\overline{0},\overline{3}\rangle$
2257	61×37	3	4	13	18	24	41	$\langle\overline{0},\overline{1}\rangle$
						36	31	$\langle\overline{0},\overline{3}\rangle$
2561	197×13	23	1	93	6	40	31	$\langle\overline{0},\overline{3}\rangle$
						44	25	$\langle\overline{0},\overline{1}\rangle$
2873	221×13	26	1	105	6	32	43	$\langle\overline{0},\overline{3}\rangle$
						52	13	$\langle\overline{0},\overline{1}\rangle$
						8	53	$\langle\overline{0},\overline{1}\rangle$
2977	229×13	27	1	109	6	36	41	$\langle\overline{0},\overline{1}\rangle$
						24	49	$\langle\overline{0},\overline{1}\rangle$

TABLE 4.3: $< s,t >$ class pair $< \overline{1},\overline{2} >$

m	Factors	r_1	r_0	s	t	x	y	$\langle x, y \rangle$ class pair
697	41×17	3	2	13	8	16	21	$\overline{0},\overline{1}$
						24	11	$\overline{0},\overline{3}$
1241	73×17	7	2	29	8	4	35	$\overline{0},\overline{3}$
						20	29	$\overline{0},\overline{1}$
1513	89×17	9	2	37	8	28	27	$\overline{0},\overline{3}$
						12	37	$\overline{0},\overline{1}$
1649	97×17	10	2	41	8	40	7	$\overline{0},\overline{3}$
						32	25	$\overline{0},\overline{1}$
1921	113×17	12	2	49	8	20	39	$\overline{0},\overline{3}$
						36	25	$\overline{0},\overline{1}$
2329	137×17	15	2	61	8	48	5	$\overline{0},\overline{1}$
						40	27	$\overline{0},\overline{3}$
3281	193×17	22	2	89	8	16	55	$\overline{0},\overline{3}$
						40	41	$\overline{0},\overline{1}$

TABLE 4.4: $< s, t >$ class pair $< \overline{1},\overline{0} >$

	$< x, y > = < \overline{0}, \overline{1} >$				$< x, y > = < \overline{0}, \overline{3} >$			
	R_0 even		R_0 odd		R_0 even		R_0 odd	
$R_1{}'$	R_1	q_{e1}	R_1	q_{01}	R_3	q_{e3}	R_3	q_{03}
$\overline{0}$	$\overline{0}$	1	$\overline{2}$	9	$\overline{3}$	15	$\overline{1}$	7
$\overline{1}$	$\overline{3}$	13	$\overline{1}$	5	$\overline{0}$	3	$\overline{2}$	11
$\overline{2}$	$\overline{2}$	9	$\overline{0}$	1	$\overline{1}$	7	$\overline{3}$	15
$\overline{3}$	$\overline{1}$	5	$\overline{3}$	13	$\overline{2}$	11	$\overline{0}$	3

TABLE 4.5: Some class relationships

(a)

	y^*	1	9	5	7	3
R_1'	y_0	1	9	5	17	13
	$\bar{t}_0$	0,4	6,2	3,7	4,0	1,5
$\overline{0}$ or $\overline{2}$		2,6	0,4	5,1	6,2	3,7
	$\bar{t}_0$	5,1	3,7	0,4	1,5	6,2
$\overline{1}$ or $\overline{3}$		7,3	5,1	2,6	3,7	0,4

(b)

R_1'	y^*	1	9	5	7	3
	y_0	11	19	15	7	3
	$\bar{t}_0$	3,7	1,5	6,2	0,4	5,1
$\overline{0}$ or $\overline{2}$		5,1	3,7	0,4	2,6	7,3
	$\bar{t}_0$	6,2	4,0	1,5	3,7	0,4
$\overline{1}$ or $\overline{3}$		0,4	6,2	3,7	5,1	2,6

TABLE 4.6: $< x, y >$ class pairs : (a) $< \overline{0}\,\overline{1} >$, (b) $< \overline{0}\,\overline{3} >$

Substituting this value of r_i into equation (4.4) we see that

$$R_1{}' = r_j \tag{4.5}$$

thus,

$$p = 4(2R_1{}') + 1, \tag{4.6}$$

which is consistent with p being in class $\overline{1}$ and in an even row.

The class relationships between the rows for $y = 4R_1 + 1$ ($< x, y >$ pair $< \overline{0}, \overline{1} >$) and $y = 4R_3 + 3$ ($< x, y >$ pair $< \overline{0}, \overline{3} >$) and the quantity $R_1{}'$ are shown in Table 4.5. These are more complex than for the odd row case (Sections 2 and 3). However, since equations (3.7) to (3.11) still apply and the values of y_0 and $\bar{t}_0$ in Table 3.3 (for $< x, y >$ $< \overline{0}, \overline{3} >$) and Table 3.4 (for $< x, y >$ $< \overline{0}, \overline{1} >$) apply (Table 4.6), the procedure for estimating x and y is the same as before, except that two $\bar{r}_i$ values have to be considered instead of one. Since the maximum $y = (n-4)^{\frac{1}{2}}$ only a few $\bar{t}_0$ values need to be considered, unless n is very large, so that the calculation of $< x, y >$ class couples is very rapid.

As an example, consider the two non-primes for $< x, y > = < \overline{0}, \overline{3} >$, 833 and 2009 mentioned above. These fall in the $< s, t >$ class pair $< \overline{1}, \overline{3} >$. Data used are from Tables 3.2 and 4.6. Consider 833 in Table 4.7.

Class of $< x, y >$	n^*	Class of R_1'	Max y	$y* = 7$		$y* = 3$	
$\overline{0}, \overline{3}$	3	$\overline{0}$	27	$y_0 = 7$	y	$y_0 = 3$	y
				$\bar{t}_0$ 0, 4	7	$\bar{t}_0$ 5, 1	23
				2, 6	–	7, 3	–
$\overline{0}, \overline{1}$				$y_0 = 17$		$y_0 = 13$	
				$\bar{t}_0$ 4, 0	17	$\bar{t}_0$ 1, 5	–
				6, 2	–	3, 7	–

TABLE 4.7: Example with 833.

There are three possible values of y, namely 7, 17, and 23, but only 7 gives an integer value for x, that is, 28.

For $m = 2009$, there are 7 possible values for y, namely $35, 27, 3, 43, 5, 37,$ and 13. However, only 35 gives an integer value for x, that is, 28. Whilst these non-primes have a unique $< x, y >$ value, x and y have a common factor, 7, which shows that m cannot be a prime.

The results here parallel those for the odd row case (Sections 2 and 3) with $< s, t >$ classes $< \overline{1}, \overline{1} >$ and $< \overline{1}, \overline{3} >$ being similar to $< \overline{3}, \overline{1} >$ and $< \overline{3}, \overline{3} >$ in that the non-primes do not have multiple values of x and y, but have a common factor for x and y. As can be seen from Table 2.1, the different characteristics occur when both s and t are odd in contrast to s and t being odd, even, respectively.

5. FINAL COMMENTS

We have analysed the number structure of Class $\overline{1}$ in the modular ring $\mathbb{Z}_4$ in detail and this has shown up the characteristics of primes in this ring so that they can be easily identified directly.

In summary, when given an integer in class $\overline{1}$ that is prime to 3 and 5 and not a square, one first determines whether the integer is in an odd or even row within class $\overline{1}$. If in an odd row, it will follow $(8R_3{}' + 5)$, and $R_3{}'$ can be easily calculated so that the class of the rows $(\overline{r}_i)$ of y (the odd component in the $< x, y >$ pair) can be deduced from Table 3.1 and $y_0, \bar{t}_0$ obtained from Table 3.4 using $n^*, y*$ data from Table 3.2. Hence possible y values can be estimated. If $(n - y^2)^{\frac{1}{2}}$ is an integer, then the y is acceptable. If only one value of the $< x, y >$ pair is obtained and x, y have no common factors, then the integer must be a prime (see Tables 3.5-3.7).

If the integer lies in an even row it will follow $(8R_1{}' + 1)$ so that $R_1{}'$ can easily be determined, and hence y_0 and $\bar{t}_0$, and thence y can be found for Table 4.6 using $y*$ from Table 3.2. If $(n - y^2)^{\frac{1}{2}}$ is integer than the y value is acceptable. The same criteria as for the odd row applies for a prime (see Table 4.7).

The number of possible y values will naturally increase as n increases. The worst case will be when $y*$ has three values (n^* is 1 or 9) and the row for the integer is even in class $\bar{1}$. In this case, for an integer of the order of 10^6 the maximum number of possible y values will be 72 for each of the $< x, y >$ pairs $< \bar{0}, \bar{1} >$ and $< \bar{0}, \bar{3} >$. For example, 1014721 has only one y value that gives an integer x (even though there are 144 possible values for y). Since x, y have no common factors, this integer is therefore a prime with $< x, y >$ in $< \bar{0}, \bar{1} >$ and $x = 660, y = 761$.

For the best case, when the integer falls in an odd row in class $\bar{1}$ with $n^* = 3$ of 7, there are only two values of $y*$ and twenty-six possible values of y in each of $< x, y > = < \bar{2}, \bar{1} >$ and $< x, y > = < \bar{2}, \bar{3} >$.

For example, 1014733 has no values of y that yield an integer x and hence is a non-prime that must fall in $< s, t >$ class pair $< \bar{3}, \bar{1} >$ or $< \bar{3}, \bar{3} >$. Thus the factors will be $11, 19, 43, \ldots$ or $7, 23, 31, \ldots$. The factors are 19 and 53407 (both primes) so that 1014733 falls in $< s, t > = < 3, 1 >$ and $s = 26695$, $t = 9$.

The main result here is that a single value of $< x, y >$, when x and y have no common factors, indicates a prime. Faster methods of estimating x and y can always be used (if available) for very large integers. In such cases the interested reader could see [3] for recent algorithmic advancements.

REFERENCES

1. J.V. Leyendekkers, J.M. Rybak and A.G. Shannon, Analysis of Diophantine Properties using Modular Rings with Four and Six Classes. Notes on Number Theory and Discrete Mathematics 3, 2, 1997, 61-74.

2. J.V. Leyendekkers, J.M. Rybak, The generation and analysis of Pythagorean triples within a two-parameter grid. *International Journal of Mathematical Education in Science and Technology,* 26,(6),1995: 787-793.

3. Richard E. Crandall, The challenge of large numbers, *Scientific American,* 276(2),1997:58-62.