NNTDM 9 (2003), 3, 49-58

SOME CHARACTERISTICS OF PRIMES WITHIN MODULAR RINGS

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

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

Abstract

The squares of primes in the Modular Ring Z_4 fall in even rows, R_1, in Class $\bar{1}_4$ with $R_1 = 6K_j$ and $K_j = \frac{1}{2}n(3n \pm 1)$ (depending on the parity of *j*). The *n* values are found to equal the rows that the primes occupy when Z_6 is set as a tabular array. The primes in Z_4 equal a unique sum or difference of squares $(x^2 \pm y^2)$ and via *n*, the (*x*,*y*) pairs can be identified within the Z_6 structure. The *n* values for composites follow well-defined linear functions that permit easy sorting. Finally, the parameter $\underline{n}$ in the well-known function $\underline{P} = h2^{\underline{n}} - 1$ has been identified as the row in one or more of the Modular Rings Z_{10}, Z_6 or Z_4 that contains one or more primes.

1. Introduction

Historically in the study of primes, the main objectives have been to identify primes and an associated study has been to find their distribution and number, and the factorisation of large numbers. Although it is well-known that primes can have forms such as $(4r+1),(4r+3)$, and $(6r-1),(6r+1)$, and so on, which allow further categorisation of these integers, the significance of any such relationships can only be understood in the context of the structure of the integers as a whole. This can be conveniently explored by using Modular Rings. Here we use three rings, Z_4, Z_6, Z_{10}. A number of related studies of primes within modular rings have already been made [1,2,3,4,5,6,7]. Each ring contains all the integers, partitioned into classes.

Initially, we look at the squares of primes within the ring Z_4. Squares and the row structures of squares are well understood for this modular ring [8]. Details of the rings have been given previously [9,10], so we merely give a brief summary of them here. The four classes of Z_4 are given by $(4r_i + i)$ in which $\bar{i}$ is the Class and r_i is the row in a tabular array of $\bar{i}$. Obviously, even integers $\in \{\bar{0}_4, \bar{2}_4\}$ and odd integers $\in \{\bar{1}_4 \bar{3}_4\}$. There are no powers in $\bar{2}_4$ and no even powers in $\bar{3}_4$.

Integers in Z_6, which has six classes, are given by $(6r_i + (i-3))$ (Table 1). Of the three classes, $\bar{2}_6, \bar{4}_6$ and $\bar{6}_6$ which contain odd integers, Class $\bar{2}_6$ contains no even powers, while Class $\bar{6}_6$ contains only those integers *N* such that $3|N$.

Row ↓ *Class* →	$\bar{1}_6$	$\bar{2}_6$	$\bar{3}_6$	$\bar{4}_6$	$\bar{5}_6$	$\bar{6}_6$
0	-2	-1	0	1	2	3
1	4	5	6	7	8	9
2	10	11	12	13	14	15
3	16	17	18	19	20	21
4	22	23	24	25	26	27

Table 1: Array of Z_6

Integers in the ten classes, $\bar{i} \in Z_{10}$ are given by $(10r_i + i)$. For this ring, the right end digits (REDs) are all the same for a given Class; that is, integers in $\bar{3}_{10}$ all end in 3, and so on.

2. Squares in Z_4

Within the modular ring Z_4, squares of odd integers fall in very well defined rows and only in the Class $\bar{1}_4$. It is of interest therefore to examine the row structure of the squares of primes to see whether such structure can provide further evidence of how primes are distributed, and thus give more depth to prime characterisation.

The odd squares are given by $4R_1 + 1$ and the row is always even, with $6|R_1$, unless 3|N [8]. Since we are only concerned with primes here, the square will fall in rows given by

$$R_1 = 6K_j, \quad j = 0,1,2,3, \tag{2.1}$$

where K_j is a generalized pentagonal number defined by

$$K_j = \begin{cases} \frac{1}{2}n(3n-1), & even\, j, \\ \frac{1}{2}n(3n+1), & odd\, j, \end{cases} \tag{2.2}$$

with *n*=1,2,3,.. [8,12]. This yields

$$n = \begin{cases} \frac{1}{2}(j+2), & even\, j, \\ \frac{1}{2}(j+1), & odd\, j. \end{cases} \tag{2.3}$$

Thus in Z_4,

$$\begin{aligned} p_j^2 &= 24K_j + 1 \\ &= 6(6n_1^2 - 2n_1) + 1 \end{aligned} \tag{2.4}$$

when

$$K_j = \tfrac{1}{2}n_1(3n_1 - 1).$$

This is equivalent to a prime in Class $\bar{2}_6$ ($\in Z_6$) being squared; that is,

$$(6r_2 - 1)^2 = 6(6r_2^2 - 2r_2) + 1, \tag{2.5}$$

so that

$$n_1 = r_2.$$

Hence all primes with $K = \frac{1}{2}n_1(3n_1 - 1) \in Z_4$ would occur in $\bar{2}_6 \in Z_6$. As with Z_4, so too in Z_6 odd squares ($3 \nmid N$) are confined to one Class, namely $\bar{4}_6$, as can be seen from Equation (2.5).

Similarly, if

$$K_j = \frac{1}{2}n_2(3n_2 + 1),$$

then the prime will occur in a site in $\bar{4}_6 \in Z_6$ since, in this case

$$24K_j + 1 = 6(6n_2^2 + 2n_2) + 1, \tag{2.6}$$

and

$$(6r_4 + 1)^2 = 6(6r_4^2 + 2r_4) + 1. \tag{2.7}$$

Table 2 lists differences between composites and primes in terms of constraints on Right End Digits (REDs).

Ring	Integer type	Row* of square	K*	n_1^* n_2^*
Z_4	prime $\neq 5$	0 or 2	0,2,5,7	$\neq 1,6$ $\neq 4,9$
	composite 3 does not divide N	0,2,6	0,1,2,5,6,7	0,1,2,3,4,5,6,7,8,9
Z_6	prime	0 or 8		
	composite	0,4,8		

Table 2: Right End Digit (RED) Constraints on Various Rows & Parameters

Primes from both Classes $\bar{1}_4$ and $\bar{3}_4$ contribute to n_1 and n_2 but the parity of n indicates the Class of the prime (Table 3).

F(n)	Class of *p*	Parity of *n*
½n(3n-1)	$\bar{1}_4$	odd
	$\bar{3}_4$	even
½n(3n+1)	$\bar{1}_4$	even
	$\bar{3}_4$	odd

Table 3: Class and Parity

Primes in Class $\bar{1}_4$ equal a sum of squares $(x^2 + y^2)$ [1]. In contrast to composite integers, there is only one value for x and y which have opposite parity and no common factors. When n_1 is odd and n_2 is even, the corresponding primes are from Class $\bar{1}_4$ (Table 3). Hence, for these n values:

$$6n_1 - 1 = x^2 + y^2, \quad (n_1 \text{ odd}), \tag{2.8}$$

so that

$$n_1 = \tfrac{1}{6}\left(x^2 + y^2 + 1\right), \tag{2.9}$$

and

$$6n_2 + 1 = x^2 + y^2, \quad (n_2 \text{ even}), \tag{2.10}$$

and

$$n_2 = \tfrac{1}{6}\left(x^2 + y^2 - 1\right) \tag{2.11}$$

Primes in Class $\bar{3}_4$ equal a difference of squares $\left(x^2 - y^2\right)$, with x,y a unique pair, unlike composites which have multiple pairs [2]. For this Class, n_1 is even and n_2 odd (Table 3), and

$$6n_1 - 1 = x^2 - y^2, \tag{2.12}$$

so that

$$n_1 = \tfrac{1}{6}\left(x^2 - y^2 + 1\right), \quad (n_1 \text{ even}), \tag{2.13}$$

and

$$n_2 = \tfrac{1}{6}\left(x^2 - y^2 - 1\right), \quad (n_2 \text{ odd}). \tag{2.14}$$

In this way, rows containing primes in the modular ring Z_6 may be equated to functions from the modular ring Z_4. Table 4 lists values of n_1 for primes in the range 5≤p≤1013. A similar set can be generated for n_2 (being the set of rows containing primes in Class $\bar{4}_6$).

Values of n from $F(n) = \frac{1}{2}n(3n-1)$ [n = row for primes $\in \bar{2}_6$]
1,2,3,4,5,7,8,9,10,12,14,15,17,18,19,22,23,25,28,29,30,32,33, 38,39,40,42,43,44,45,47,49,52,53,58,59,60,64,65,67,70,72,74, 75,77,78,80,82,84,85,87,93,94,95,98,99,100,103,107,108,109, 110,113,114,117,120,124,127,129,133,135,137,138,140,143, 144,147,148,152,155,157,158,159,162,163,164,169

Table 4: Values of n_1 for primes in the range 5≤p≤1013.

The missing n values in Table 4 (6,11,13,...) belong to composite integers and follow an equation of the form

$$n_1 = a_0 + pd, \tag{2.15}$$

where p is a prime and $a_0 \in Z$ for a given p, with d=0,1,2,2,3,4,... .The values of $p - a_0$ equal the rows of the prime $p \in Z_6$ (Table 5). When $p \in \bar{2}_6, (p - a_0) < 0$ (Table 5). Thus,

$$6n_1 = 1 + (5 + 6d)p, \quad \left(p \in \bar{4}_6\right),$$

or

$$6n_1 = 1 + (7 + 6d)p, \quad \left(p \in \bar{2}_6\right)$$

A sieving method could be used to find n values corresponding to primes (Figure 1). A simpler method along these lines has been used to identify twin primes [5,7].

p	Row	Class	$p-a_0$
7	1	$\bar{4}_6$	1
11	2	$\bar{2}_6$	-2
13	2	$\bar{4}_6$	2
17	3	$\bar{2}_6$	-3
19	3	$\bar{4}_6$	3
23	4	$\bar{2}_6$	-4
29	5	$\bar{2}_6$	-5

Table 5: Values of $p-a_0$

3. Primes from $\underline{P} = h2^n - 1$

Riesel [11] gives extensive tables of n,h combinations that produce primes from $(h2^n \pm 1)$. Here we consider only ($h2^n - 1$), since the same analysis can be applied to $(h2^n + 1)$.

Many of the n sequences for a given h can be found in the array of Table 4, and since these n represent rows in Z_6 which contain primes, the following question arises: Are the n values of the $(h2^n - 1)$ actually prime-containing rows in modular rings?

As can be seen from Table 6, they are. It is found that all n (except in the very high range) identify rows which contain one or more primes. Predominantly these rows occur in Z_6 and Z_{10} and occasionally in Z_4. For Z_6 the primes are given by

$$p = 6n \pm 1 \tag{3.1}$$

so that if $\underline{P}$ represents the prime from the (h,n) function, then

$$\ln(\underline{P}+1) = \ln\left(2^{1/6} h\right) + (1/6)(\ln 2)p, \ (p \in \bar{2}_6), \tag{3.2}$$

and

$$\ln(\underline{P}+1) = \ln\left(2^{-1/6} h\right) + (1/6)(\ln 2)p, \ (p \in \bar{4}_6). \tag{3.3}$$

Similar log-linear relationships occur in the corresponding cases for Z_4 or Z_{10}. For a given h, then, the derived primes P are simply related to the primes in row n of one of these three modular rings.

Table 7 illustrates the Ring and Class distribution pattern of rows which contain primes for different h values. In general, when h is a prime the number of values of n are less than for composite h. Only h=181, 199 have more than 30 valid n.

Table 8 lists n values which do not correspond to rows which contain primes in any of these three modular rings. However, in most cases (75%), when $n \pm 1$ or $n \pm 2$ are taken as the rows, these contain primes in either Z_6 or Z_{10}. It seems that the linearity of Equations (3.2) and (3.3) becomes unstable at these large n values.

n=row	No. of h which contain n	i (for Z_i)	Class	Primes
1	37	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{1}_{10}, \bar{7}_{10}$	5,7 11,17
2	37	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{3}_{10}, \bar{9}_{10}$	11,13 23,29
3	35	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{1}_{10}, \bar{7}_{10}$	17,19 31,37
4	28	6 10	$\bar{2}_6$ $\bar{1}_{10}, \bar{3}_{10}, \bar{7}_{10}$	23 41,43,47
5	31	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{3}_{10}, \bar{9}_{10}$	29,31 53,59
6	21	6 10	$\bar{4}_6$ $\bar{1}_{10}, \bar{7}_{10}$	37 61,67
7	20	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{1}_{10}, \bar{3}_{10}, \bar{9}_{10}$	41,43 71,73,79
8	20	6 10	$\bar{2}_6$ $\bar{3}_{10}, \bar{9}_{10}$	47 83,89
9	20	6 10	$\bar{2}_6$ $\bar{7}_{10}$	53 97
10	20	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{1}_{10}, \bar{3}_{10}, \bar{7}_{10}, \bar{9}_{10}$	59,61 101,103,107,109
11	21	6 10	$\bar{4}_6$ $\bar{3}_{10}$	67 113
12	16	6 10	$\bar{2}_6, \bar{4}_6$ $\bar{7}_{10}$	71,73 127

Table 6: Rows which contain at least one prime

	Z_6		Z_{10}*	Z_4*
h	$\bar{2}_6$	$\bar{4}_6$	$\bar{i}_{10}$	$\bar{i}_4$
3	1,2,3,4,7,18,38, 43,64,94,103, 143,470,1274	1,2,3,6,7,11,18,38, 55,76,103,143,206, 216,391,458	306, 12676 $(\bar{1}_{10})$ 827 $(\bar{3}_{10})$	324 $(\bar{1}_4)$
15	1,2,4,5,10,14,17, 80,82,157,172,	1,2,5,10,17,73,125, 172,202,266,293,	224 $(\bar{3}_{10})$	1004 $(\bar{3}_4)$

	289,463	1246	2431 $(\bar{7}_{10})$	
27	1,2,4,5,8,10,14,28, 38,70,170,329,485, 500,892,1580	1,2,5,10,37,38,70, 121,122,170,500	160, 253 $(\bar{1}_{10})$ 362 $(\bar{3}_{10})$ 454 $(\bar{7}_{10})$ 574 $(\bar{1}_{10},\bar{3}_{10},\bar{9}_{10})$	
181	3,5,7,9,17,23,43, 47,85,267,653, 4783	3,5,7,11,17,23,35,47, 83,99,101,195,363, 391,623,653,1091, 1147	281 $(\bar{9}_{10})$ 519 $(\bar{7}_{10})$ 673 $(\bar{3}_{10},\bar{7}_{10})$ 701 $(\bar{3}_{10},\bar{9}_{10})$ 5345 $(\bar{3}_{10})$	

Table 7: n=row of prime(s) in $i \in Z_i$

* only calculated when Z_6 row, n, has no primes; (see Table 6)

h	n	n'	n-n'	Ring for n' Z_6	Z_{10}	Class of prime in row n'
3	3276	3280	-4	√		$\bar{4}_6$
		3277	-1		√	$\bar{1}_{10}$
	4204	4205	-1	√		$\bar{2}_6$
		4201	-3		√	$\bar{3}_{10}$
	5134	5135	-1	√		$\bar{2}_6$
		5132	2		√	$\bar{9}_{10}$
	7559	7556	3	√		$\bar{4}_6$
		7557	2		√	$\bar{1}_{10}$
15	2066	2067	-1	√		$\bar{2}_6$
		2064	2		√	$\bar{1}_{10}$
	2705	2709	-4	√		$\bar{2}_6$
		2701	4		√	$\bar{7}_{10}$
		2709	-4		√	$\bar{1}_{10}$
	4622	4625	-3	√		$\bar{4}_6$
		4626	-4		√	$\bar{1}_{10}$
	5270	5268	2	√		$\bar{2}_6$
		5269	1		√	$\bar{7}_{10}$
	7613	7616	-3	√		$\bar{4}_6$
		7614	-1		√	$\bar{7}_{10}$
27	2642	2636	6	√		$\bar{4}_6$

		2647	-5	√	$\bar{9}_{10}$
	2708	2709	-1	√	$\bar{2}_{6}$
		2703	5	√	$\bar{1}_{10}$
	4505	4503	2	√	$\bar{2}_{6}$
		4506	-1	√	$\bar{1}_{10}$
181	1565	1562	3	√	$\bar{4}_{6}$
		1566	-1	√	$\bar{7}_{10}$
	3273	3277	-4	√	$\bar{2}_{6}$
		3271	2	√	$\bar{7}_{10}$
	3661	3659	2	√	$\bar{9}_{10}$
		3666	-5	√	$\bar{4}_{6}$
	3923	3918	5	√	$\bar{4}_{6}$
		3920	3	√	$\bar{9}_{10}$
	4127	4130	-3	√	$\bar{4}_{6}$
		4124	3	√	$\bar{3}_{10}$
	5267	5262	5	√	$\bar{4}_{6}$
		5269	-2	√	$\bar{7}_{10}$
	5747	5750	-3	√	$\bar{4}_{6}$
		5749	-2	√	$\bar{3}_{10}$

Table 8: Values of *n* which do not correspond with rows which contain primes

4. Concluding Remarks

As has been shown in our previous studies [1-7], functions which involve primes are usually Class specific. Hence, a greater understanding of primes and their distribution can be obtained when integer structure is taken into account.

References

1. J. V. Leyendekkers, J.M. Rybak & A. G. Shannon. The Characteristics of Primes and Other Integers within the Modular Ring Z_4 and in Class $\bar{1}_4$. *Notes on Number Theory & Discrete Mathematics.* **4(1)** 1998: 1-17.
2. J. V. Leyendekkers, J.M. Rybak & A. G. Shannon. The Characteristics of Primes and Other Integers within the Modular Ring Z_4 and in Class $\bar{3}_4$. *Notes on Number Theory & Discrete Mathematics.* **4(1)** 1998: 18-37.
3. J. V. Leyendekkers & A. G. Shannon. An Analysis of Mersenne-Fibonacci and Mersenne-Lucas Primes. *Notes on Number Theory & Discrete Mathematics.* **5(1)** 1999: 1-26.
4. J. V. Leyendekkers & A. G. Shannon. The Goldbach Conjecture Primes within a Modular Ring. *Notes on Number Theory & Discrete Mathematics.* **6(4)** 2000: 101-112.

5. J. V. Leyendekkers & A. G. Shannon. Twin Primes and the Modular Ring Z_6. *Notes on Number Theory & Discrete Mathematics.* **7(4)** 2001: 115-124.
6. J. V. Leyendekkers & A. G. Shannon. An Analysis of Twin Primes $h2^n - 1$ Using Modular Rings Z_6 and Z_4 *Notes on Number Theory & Discrete Mathematics.* **7(1)** 2001:21-28.
7. J. V. Leyendekkers & A. G. Shannon. A Note on Twin Primes and the Modular Ring Z_6. *International Journal of Mathematical Education in Science & Technology.* **33(2)** 2002: 303-306.
8. J. V. Leyendekkers & A. G. Shannon. Powers as a Difference of Squares: The Effect on Triples. *Notes on Number Theory & Discrete Mathematics.* **8(3)** 2002: 95-106.
9. J. V. Leyendekkers, J. M. Rybak & A. G. Shannon. Integer Class Properties Associates with an Integer Matrix. *Notes on Number Theory & Discrete Mathematics.* **1(2)** 1995: 53-59.
10. 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.
11. Hans Riesel. *Prime Numbers and Computer Methods for Factorization. Progress in Mathematics, Volume 126.* Boston: Birkhäuser, 1994.
12. A. H. Beiler. *Recreations in the Theory of Numbers.* New York: Dover, 1964.

AMS Classification Numbers: 11A07, 11A41

↓Rows\Class→	1	2	3	4	5	6
0	-	-	-	1	2	3
1	4	5	6	7	8	9
2	10	11	12	13	14	15
3	16	17	18	19	20	21
4	22	23	24	25	26	27
5	28	29	30	31	32	33
6	34	35	36	37	38	39
7	40	41	42	43	44	45
8	46	47	48	49	50	51
9	52	53	54	55	56	57
10	58	59	60	61	62	63
11	64	65	66	67	68	69
12	70	71	72	73	74	75
13	76	77	78	79	80	81
14	82	83	84	85	86	87
15	88	89	90	91	92	93
16	94	95	96	97	98	99
17	100	101	102	103	104	105
18	106	107	108	109	110	111
19	112	113	114	115	116	117
20	118	119	120	121	122	123
21	124	125	126	127	128	129
22	130	131	132	133	134	135
23	136	137	138	139	140	141
24	142	143	144	145	146	147
25	148	149	150	151	152	153
26	154	155	156	157	158	159
27	160	161	162	163	164	165
28	166	167	168	169	170	171
29	172	173	174	175	176	177
30	178	179	180	181	182	183
31	184	185	186	187	188	189

Figure 1: m-value sieve for primes in Class $\bar{2}_6$: underlined values are *n* values for primes

Legend: *p*=5 *p*=7
p=11 *p*=13 *p*=17
p=19 *p*=23 *p*=29