NNTDM 7 (2001) 1, 21-28

An Analysis of Twin Primes $h2^n - 1$ Using Modular Rings $\mathbb{Z}_6$ and $\mathbb{Z}_4$

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

Twin primes of the form $h2^n - 1$ are analysed within the modular ring $\mathbb{Z}_6$. The values of h are odd and $3|h$ for the lowest valued twin prime, p_2. The other values of h fall in either the second ($\overline{2}_6$) or fourth ($\overline{4}_6$) class of $\mathbb{Z}_6$, depending on the parity of n. Functional relationships are developed for the various h, n and rows within $\mathbb{Z}_6$. All p_2 fall in class $\overline{2}_6$ and the larger prime of the twin pair, p_4, always falls in class $\overline{4}_6$. With $n_2 = 1$ and $n_4 > 1$, p_2 falls in class one ($\overline{1}_4$) of the modular ring $\mathbb{Z}_4$ and hence equals a unique set of squares ($x^2 + y^2$). Analysis of the distribution of the (x,y) pair reveals an interesting prime sequence related to the Fibonacci sequence.

1. Introduction

For more than forty years twin primes have been represented by the forms $(6r \pm 1)2^{2n-1} - 1$ (Riesel, 1956; Williams and Zarnke, 1972). The terms $(6r - 1)$ and $(6r + 1)$ are identified as integers in the classes $\overline{2}_6$ and $\overline{4}_6$ of the modular ring $\mathbb{Z}_6$, where r is used to represent the row in a tabular representation of the ring (Leyendekkers *et al*, 1995, 1997). Integers in $\mathbb{Z}_6$ are represented by $(6r_i + (i - 3))$ where $\overline{i}$ is the class. Odd integers also fall in $\mathbb{Z}_6$, given by $(6r_6 + 3)$ and in recent tabulations (Riesel, 1994) the more general form $h2^n - 1$ is used, with $h \in \{\overline{2}_6, \overline{4}_6, \overline{6}_6\}$.

Twin primes are given by $((6R_2 - 1), (6R_4 + 1))$; that is, they fall in classes $\overline{2}_6$ and $\overline{4}_6$ with $R_2 = R_4$. The upper case R is used here to identify the twin-prime rows. (Niven and Zuckerman (1972) describe how to "translate" the language and notation of set theory into that of number theory.)

In the present paper we look at the characteristics of the various h, n values of the twin primes and their interrelationships. Such information will be valuable in the study and identification of twin primes. As well, the patterns of distribution of associated variables reveal unusual prime sequences not previously studied.

2. Twin Primes of the Form $2^n h - 1$

Primes in Class $\overline{2}_6$, when put in the form $2^{n_2} h_2$ always have $h_2 \in \overline{6}_6$, that is, $3|h_2$. On the other hand, primes in Class $\overline{4}_6$ have h_4 values that fall in either $\overline{2}_6$ or $\overline{4}_6$.

Table 1 lists values of h, n for twin primes in the first 500 rows of the $\mathbb{Z}_6$ modular ring. (In each cell, the first pair is from $\overline{2}_6$ and the second from $\overline{4}_6$; within each pair the first element represents h and the second element represents n.)

3,1	3,2	9,1	15,1	21,1	15,2	9,3	51,1	27,2
1,3	7,1	5,2	1,5	11,2	31,1	37,1	13,3	55,1
69,1	75,1	45,2	3,6	99,1	57,2	15,4	135,1	141,1
35,2	19,3	91,1	97,1	25,3	115,1	121,1	17,4	71,2
39,3	87,2	105,2	27,4	231,1	261,1	285,1	75,3	309,1
157,1	175,1	211,1	217,1	29,4	131,2	143,2	301,2	155,2
321,1	165,2	405,1	411,1	207,2	429,1	441,1	255,1	129,3
161,2	331,1	203,2	103,3	415,1	215,2	221,2	511,1	517,1
525,1	531,1	273,2	9,6	615,1	639,1	645,1	651,1	165,3
263,2	133,3	547,1	577,1	77,4	5,8	323,2	163,3	661,1
357,2	363,2	741,1	93,4	405,2	417,2	849,1	861,1	447,2
715,1	727,1	371,2	745,1	881,1	835,1	425,2	431,2	895,1
117,4	939,1	483,2	975,1	999,1	507,2	1041,1	261,3	33,6
937,1	235,3	967,1	61,5	125,4	1015,1	521,2	1045,1	1057,1
1065,1	1071,1	1119,1	567,2	585,2	1191,1	1275,1		
533,2	67,5	35,6	1135,1	1171,1	149,4	319,3		
81,5	1329,1	21,7	339,3	1365,1	1395,1	1401,1	1485,1	375,3
1297,1	665,2	1345,1	1357,1	683,2	349,3	701,2	743,2	1501,1

Table 1: h,n characteristics of twin primes for the first 500 rows of $\mathbb{Z}_6$
$p = 2^n h - 1$.1st rows: $p \in \overline{2}_6$; 2nd rows $p \in \overline{4}_6$.

Since any integer >5, with the right end digit (RED) equal to 5, cannot be a prime, the first prime of the twin cannot have RED=3, whilst the second prime of the twin cannot have RED=7. Consequently, this imposes constraints on the REDs (indicated by an asterisk) of h (or h^*) and on $(2^n)^*$. That is

$$(h_2^*, (2^{n_2})^*) \notin \{(1,4),(3,8),(7,2),(9,6)\},$$

and

$$(h_4^*, (2^{n_4})^*) \notin \{(1,8),(3,6),(7,4),(9,2)\}.$$

Furthermore, since $p_2^*, p_4^* \neq 5$, then

$$\{(h_2^*, (2^{n_2})^*), (h_4^*, (2^{n_4})^*)\} \cap \{(1,6),(3,2),(7,8),(9,4)\} = \emptyset.$$

These constraints are reflected in Table 1. For example, except for $p_2 = 5$, when $n_2 = 1, h_2^* \neq 3,7$; when $n_2 = 2, h_2^* \neq 1,9$. If $n_4 = 1, h_4^* \neq 3,9$, and so on.

Since either $n_2 = 1$ or $n_4 = 1$, there are two (h,n) groups, as in Table 2.

Group	Characersitics	Relationships¤
I	$h_4 > h_2; n_2 > n_4 = 1$	$h_4 = 2^{n_2-1}h_2 + 1$
II	$h_2 > h_4; n_4 > n_2 = 1$	$h_2 = 2^{n_4-1}h_4 - 1$

Table 2: (h,n) groups; ¤ derived from $p_4 - p_2 = 2$

Since $3|h_2$,

$$h_2 = 3(2t + 1) \tag{2.1}$$

and h_2 is always odd (and this yields a maximum value for n, as obviously, $(2h)2^{n-1} = h2^n$) ; as well,

$$h_4 = (2^{n_2-1}3)(2t + 1) + 1 \qquad \text{Group I,}$$

and (2.2)

$$h_4 = \frac{3t+2}{2^{n_4-2}} \qquad \text{Group II.}$$

For Group II, when $n_4 = 2, t$ is odd; but if $n_4 > 2$, t must be even. Furthermore, h_4 is always odd (Table 1). In general,

$$2^{n_4-1}h_4 = 1 + 2^{n_2-1}h_2. \tag{2.3}$$

When $n_4 = 1$ or $n_2 = 1$, the functions of Table 2 are obtained. The row in $\mathbb{Z}_6$ which contains the twin primes ($R_2 = R_4$) is simply related to n_2 and the row that h_2 occupies in $\overline{6}_6$.

With $p_2 = 6R_2 - 1 = 2^{n_2}h_2 - 1$ and since $h_2 = 6r_6 + 3$,

$$R_2 = 2^{n_2}(r_6 + ½) \tag{2.4}$$

from Equation (2.1) $r_6 \equiv t$. As well, for the twin primes $p_4 \in \overline{4}_6$,

$$p_4 = 6R_4 + 1 = 2^{n_4}h_4 - 1.$$

For Group I,

$$h_4 = 6r_4 + 1,$$

so that, with $n_4 = 1$,

$$R_4 = 2r_4, \tag{2.5}$$

and since $R_4 = R_2$, from Equation (2.4)

$$r_4 = 2^{n_2-2}(2r_6 + 1). \tag{2.6}$$

For Group II, h_4 can fall in either Class $\overline{2}_6$ or $\overline{4}_6$ (Table 3).

n_4	h_4
even	$6r_2 - 1$
odd	$6r_4' + 1$

Table 3

If we use the same methods as above, then when $h_4 \in \overline{4}_6$, $h_4 = 6r_4' + 1$,

$$R_4 = \frac{\left(2^{n_4-1}6r_4' + (2^{n_4-1} - 1)\right)}{3}, \tag{2.7}$$

while $h_4 \in \bar{2}_6$ has $h_4 = 6r_2 - 1$, so that

$$R_4 = \frac{(2^{n_4-1}6r_2 - (2^{n_4-1} + 1))}{3}. \tag{2.8}$$

More simply, For Group II (when $n_4 > 1$) R_4 may be expressed in the forms

$$R_4 = a(4r_2 - 1) + b, \ (n_4 \text{ even}), \tag{2.9}$$

or

$$R_4 = c(8r_4' + 1) + d, \ (n_4 \text{ odd}), \tag{2.10}$$

with

$$a = 2^{n_4-1} \text{ and } b = \sum_{j=0}^{n_4-4} 2^j, \ \left(n_4 = 2, b = 0, j \text{ even}\right),$$

and

$$c = 2^{n_4-3} \text{ and } d = \sum_{j=0}^{n_4-5} 2^j, \ \left(n_4 = 3, b = 0, j \text{ even}\right).$$

The above information specifically characterises the twin primes and will have obvious value for studies in the super large domain. It is of interest too that for Group II, the R_4 functions (Equations (2.7), (2.8)) appear to contain both the Mersenne number, $M_n = 2^n - 1$, and the Fermat number, $F_n = 2^n + 1$. However, the parities of n are opposite to those of M_n and F_n. This is so because both terms must be divisible by 3 and hence can never be primes.

3. Primes Sequences Associated with h, n Pairs

When $n_2 = 1$ and $n_4 > 1$, $p_2 = 2h_2 - 1$, and since $h_2 = (6r_6 + 3)$, then

$$p_2 = 12r_6 + 5 \tag{3.1}$$

or

$$p_2 = 4(3r_6 + 1) + 1. \tag{3.2}$$

Equation (3.2) shows that in the modular ring $\mathbb{Z}_4$, $p_2 \in \bar{1}_4$ within a row equal to $(3r_6 + 1)$. (Integers in $\mathbb{Z}_4$ equal $4r_i + i$, $\bar{i}$ being the class (Leyendekkers *et al*, 1997).) Thus p_2 must be a sum of squares (Leyendekkers *et al*, 1998).

From Equation (3.1), $p_4 = 12r_6 + 7 = 4(3r_6 + 1) + 3$, so that $p_4 \in \bar{3}_4$, and hence $p_4 \neq x^2 + y^2$.

With $p > 5$, $p^* \neq 5$, so that there will be constraints on the REDs of x and y. That is:

$$\{(x^2)^*, (y^2)^*\} \cap \{(0,5), (4,1), (6,9)\} = \varnothing.$$

Hence,

$$\{x^*, y^*\} \cap \{(0,5), (2,1), (2,9), (4,3), (4,7), (6,3), (6,7), (8,1), (8,9)\} = \varnothing.$$

Table 4 lists values of r_6 (or t), p_2 and the corresponding (x,y) pairs which form the squares.

r_6	$p_2 = x^2 + y^2$	(x,y)	r_6	$p_2 = x^2 + y^2$	(x,y)
0	5	(2,1)	102	1229	(2,35)
1	17	(4,1)	106	1277	(34,11)
2	29	(2,5)	107	1289	(8,35)
3	41	(4,5)	108	1301	(26,25)
8	101	(10,1)	123	1481	(16,35)
11	137	(4,11)	141	1697	(4,41)
12	149	(10,7)	143	1721	(40,11)
16	197	(14,1)	156	1877	(14,41)
22	269	(10,13)	162	1949	(10,43)
23	281	(16,5)	166	1997	(34,29)
38	461	(10,19)	173	2081	(20,41)
43	521	(20,11)	177	2129	(40,23)
47	569	(20,13)	178	2141	(46,5)
51	617	(16,19)	186	2237	(46,11)
53	641	(4,25)	198	2381	(34,35)
67	809	(28,5)	212	2549	(50,7)
68	821	(14,25)	221	2657	(16,49)
71	857	(4,29)	227	2729	(52,5)
73	881	(16,25)	232	2789	(50,17)
87	1049	(32,5)	233	2801	(20,49)
88	1061	(10,31)	247	2969	(40,37)

Table 4: $n_2 = 1, n_4 > 1$ (Group II)

With x or y constant, y or x appear to follow regular sequences. For example, when $x = 10, y = 6v + 1$ (Class $\bar{4}_6$), although values of the integer v are specific for twin primes. Those values of v not giving twin primes yield $(100 + y^2)$ values that are frequently primes or equal to $(p - 2)$ and for nearly half the first forty v values $(100 + y^2)$ either immediately precedes or follows twin primes (occasionally both). Table 5 summarises these results.

For $N < 90700$, when $N = p - 2$, y is a prime or a square or has a RED of 5. If N had been a prime in such cases, then N would have been one of a twin prime pair. Thus $N = p - 2$ might be thought of as a pseudo twin prime. Other interesting sequences probably exist within Group I where $n_4 = 1$ and $n_2 > 1$.

v	y	$N = 10^2 + y^2$	Comments	v	y	$N = 10^2 + y^2$	Comments
0	1	101 p	Twin p	30	181 p	32861	N=p-8
1	7 p	149 p	Twin p	31	187	35069 p	
2	13 p	269 p	Twin p	32	193 p	37349	N=p-8
3	19 p	461 p	Twin p	33	199 p	39701	N=p-2
4	25	725	N=p-2	34	205	42125	N=p-6
5	31 p	1061 p	Twin p	35	211 p	44621 p	Twin p
6	37 p	1469	N=p-2	36	217	47189 p	
7	43 p	1949 p	Twin p	37	223 p	49829	N=p-2
8	49	2501	N=p-2	38	229 p	52541 p	Twin p
9	55	3125	N=p+4	39	235	55325	N=p-6
10	61 p	3821 p	Twin p	40	241 p	58181	N=p-8
11	67 p	4589	N=p-2	41	247	61109	N=p+10
12	73 p	5429	N=p-2	42	253	64109 p	
13	79 p	6341	N=p-2	43	259	67181 p	
14	85	7325	N=p+4	44	265	70325	N=p-2
15	91	8381	N=p+4	45	271 p	73541	N=p-6
16	97 p	9509	N=p-2	46	277 p	76829 p	Twin p
17	103 p	10709 p	Twin p	47	283 p	80189	N=p-2
18	109 p	11981 p		48	289	83621 p	
19	115	13325	N=p-2	49	295	87125	N=p+4
20	121	14741 p		50	301	90701	N=p-2
21	127 p	16229 p	Twin p	51	307 p	94349 p	Twin p
22	133	17789 p	Twin p	52	313 p	98069	$N=p_1 - 12 = p_2 + 12$
23	139 p	19421 p	Twin p	53	319	101861	N=p-2
24	145	21125	N=p+4	54	325	105725	N=p-2
25	151 p	22901 p		55	331 p	109661 p	Twin p
26	157 p	24749 p		56	337 p	113669	N=p+12
27	163 p	26669 p		57	343	117749	N=p-2
28	169	28661 p	Twin p	58	349 p	121901	N=p-8
29	175	30725	N=p-2	59	355	126125	N=p-2
				60	361	130421	N=p-2

Table 5: p, prime

When $p > 5$, since $p^* \neq 5, v^* \neq 4,9$. As can be seen from Table 5, these REDs for v yield $N^* = 5$. Deleting $v^* = 4,9$, we get 83% of the remaining values of N equal to a prime or $p - 2$, and 43% of these are twin primes. From $v = 60$ to 100, excluding $N^* = 5$, the yield drops to 52% with only 12% twin primes. This result merely reflects the fall off in prime

population, as the overall pattern of distribution $(TP, p, p-2, p+4$, and so on$)$ is consistent. Even when $N^* = 5, N = p-2$ or $N = p+4$ are commonly found.

4. Conclusion

A detailed analysis of primes in the modular ring $\mathbb{Z}_4$ and the class $\bar{1}_4$ has been given previously (Leyendekkers *et al*, 1998).

For twin primes, when $x \in \bar{2}_4$, (that is, $x = 4r_2 + 2$, as for $x = 10$, with $r_2 = 2$), the class pair for (x,y) is either $(\bar{2}_4, \bar{1}_4)$ or $(\bar{2}_4, \bar{3}_4)$. When $y = 4r_3 + 3$ (class $\bar{3}_4$) one finds that the rows that r_3 occupies in $\mathbb{Z}_4$ have the sequence:

$$\{0, 1, 1, 2, (6,7), 8, 13, (19,20), 34, (35)\}.$$

Fibonacci nos	v	y	Character of N
0	1	7	TP
1	3	19	TP
1	5	31	TP
2	7	43	TP
3	9	55	TP+4
5	15	91	p+4 or TP-6
8	23	139	TP
13	35	211	TP
	37	223	p-2
21	57	343	p-2
34	93	559	TP
	91	547	p-2
55	147	883	p-2
	149	895	p-2

Table 6: Comparative series for $N = 10^2 + y^2, y \in \bar{3}_4$; $y = 4r_3 + 3$, TP: twin prime, p: prime

The unbracketed values are elements of the sequence of Fibonacci numbers. The analysis of rows within rows in the modular rings is interesting and often reveals underlying onion skin like patterns that provide insights into the structure of the integer system from different view points. In the present case, for the row (in which r_3 lies) to follow the Fibonacci sequence exactly, the corresponding v sequence would be that show in Table 6. Such a sequence does not always produce a prime but N is close to a twin prime or is a pseudo twin prime ($p-2$ set). Double values for v and y in Table 6 arise because the row for (r_3) falls in the same row for both y values, but in different classes.

We conclude with two recent relevant results from classical number theory. Atanassov (1999) has proved that $(p, p+2)$ are twin primes iff

$$\left\{(p-1)!\left(\frac{1}{p} + \frac{2}{p+2}\right) + \frac{1}{p} + \frac{1}{p+2}\right\} \in \mathbb{Z}_4$$

Finally we note the work of Dence and Dence (1995) who used the well-known congruence

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left\{ \begin{array}{ll} -1 \,(\mathrm{mod}\, p) & \text{if } p = 4k+1 \\ 1 \,(\mathrm{mod}\, p) & \text{if } p = 4k-1 \end{array} \right\}$$

to reduce the Clement twin criterion

$$4((p-1)! + 1) + p \equiv 0 \,(\mathrm{mod}\, p(p+2))$$

to

$$2\left(\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1\right) + 5p \equiv 0 \,(\mathrm{mod}\, p(p+2))$$

iff $(p,p+2)$ are twin primes and $p = 4k-1$, and

$$2\left(\left(\left(\frac{p-1}{2}\right)!\right)^2 - 1\right) - 5p \equiv 0 \,(\mathrm{mod}\, p(p+2))$$

iff $(p,p+2)$ are twin primes and $p = 4k+1$.

References

Atanassov, Krassimir T. 1999. *On Some of the Smarandache's Problems*. Lupton, AZ: American Research Press.

Dence, Joseph B & Dence, Thomas P. 1995. A Necessary and Sufficient Condition for Twin Primes. *Missouri Journal of Mathematical Sciences*. **7(3)**: 129-131.

Leyendekkers, JV, Rybak JM & Shannon AG. 1995. Integer Class Properties Associated with an Integer Matrix. *Notes on Number Theory & Discrete Mathematics*. **1(2)**: 53-59.

Leyendekkers, JV, Rybak JM & Shannon AG. 1997. Analysis of Diophantine Properties using Modular Rings with Four and Six Classes. *Notes on Number Theory & Discrete Mathematics*. **3(2)**: 61-74.

Leyendekkers, JV, Rybak JM & Shannon AG. 1998. The Characteristics of Primes and Other Integers within the Modular Ring $\mathbb{Z}_4$ and in Class $\overline{1}$. *Notes on Number Theory & Discrete Mathematics*. **4(1)**: 1-17.

Niven Ivan & Zuckerman Herbert S. 1972. *An Introduction to the Theory of Numbers*. New York: Wiley.

Riesel Hans. 1956. A Note on the Prime Numbers of the Forms $N = (6a+1)2^{2n} - 1$ and $M = (6a-1)2^{2n} - 1$. *Arkiv für Matematik*. **3**: 245-253.

Riesel Hans. 1994. *Prime Numbers and Computer Methods for Factorization*. Progress in Mathematics, Volume 126. Boston: Birkhäuser.

Williams HC & Zarnke CR. 1972. Some Prime Numbers of the Form $2A3^n + 1$ and $2A3^n - 1$. *Mathematics of Computation*. **26**: 995-998.

AMS Classification Numbers: 11A51, 11B39