NNTDM 16 (2010), 3, 1-10

EQUATIONS FOR PRIMES OBTAINED FROM INTEGER STRUCTURE

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

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

Abstract: Integer structure illustrates how primes represented by $4R_1+1$ are equal to a sum of squares. Such primes are in Class $\bar{1}_4 \subset Z_4$, a modular ring. The rows of squares in Z_4 are well defined and this permits equalities for the primes to be derived from the integer structure. These equalities have the forms $R_1 = r_1 + r_0$ where $r_1 = 3n(3n \pm 1)$ *or* $2 + 9n^|(n^| + 1)$ and

$$r_0 = 2^{2q}(12m(3m \pm 1) + 1) \text{ or } 2^{2q}(4(2 + 9m^|(m^| + 1)) + 1),$$

with *q* = 0, 1, 2, 3,… and *n, m* yielding the pentagonal numbers, and *n', m'* the triangular numbers. When *n* = *m* the equations are similar to Euler's prime equation. Equations for the remaining primes, in Class $\bar{3}_4$ may be obtained in the same manner using $p = y^2 - x^2$ with $(y - x) = 1$.

Keywords: primes, composites, modular rings, right-end digits, integer structure, triangular numbers, pentagonal numbers.

AMS Classification Numbers: 11A41, 11A07

1. Introduction

Fermat proved that only primes following $4r_1 + 1$ equaled a sum of squares. This follows very simply from the integer structure. We use the modular ring Z_4 since $4r_1 + 1$ represents the function for primes in class $\bar{1}_4$ of Z_4 (Table 1)

Function		$4r_0$	$4r_1+1$	$4r_2+2$	$4r_3+3$
Class		$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$
Row	0	0	1	2	3
	1	4	5	6	7
	2	8	9	10	11
	3	12	13	14	15
	4	16	17	18	19
	5	20	21	22	23
	6	24	25	26	27

Table 1

All powers of even integers fall in Class $\overline{0}_4$ whilst all even powers of odd integers fall in Class $\overline{1}_4$ [1]. Hence, with x odd and y even,

$$x^2 + y^2 = \overline{1}_4 + \overline{0}_4 = \overline{1}_4 \tag{1.1}$$

so that all odd integers equaling a sum of squares must fall in Class $\overline{1}_4$. However, for composites in Class $\overline{1}_4$, all do not equal a sum of squares, as shall be shown below.

2. Calculating *x* and *y*

(i) Right-end-digit (RED) Analysis.

To simplify the calculations we use REDs. An asterisk indicates the RED, N represents the integer (Table 2).

N*	x*	y*
1	1,5,9	0,4,6
3	3,7	2,8
7	1,9	4,6
9	3,5,7	0,2,8

Table 2

As an example, consider $N^* = 7$, then $x = 1, 11, 21, 31, 41, ...$ or $x = 9, 19, 29, 39, 49, ...$
Let

$$N - x^2 = y^2 \tag{2.1}$$

or in RED terms, 7* – 1* = 6* , then if $N - x^2$ is a square a value for y has been found and $(y^2)^* = 6^*$.

(ii) Composites versus Primes

Examples for composites in Class $\overline{1}_4$ and with $N^* = 7$, are listed in Table 3.

Only relatively few composites equal a sum of squares. As can be seen, those that do have factors in Class $\overline{1}_4$. Factors in Class $\overline{3}_4$ inhibit N from equaling a sum of squares. Note that the factors in $\overline{3}_4$ must be even since N must be in $\overline{1}_4$. That is, $\overline{3}_4\,\overline{3}_4 \subset \overline{1}_4$ or $\overline{3}_4\,\overline{3}_4\,\overline{3}_4\,\overline{3}_4 \subset \overline{1}_4$ but $\overline{3}_4\,\overline{3}_4\,\overline{3}_4 \subset \overline{3}_4$, and so on.

When only a unique (x, y) occurs x and y have a common factor. Otherwise multiple values of (x, y) occur. These characteristics distinguish the composites from primes which only have a unique set of (x, y) (Table 4). This means that an integer in $\overline{1}_4$ may be checked for primality using the $(x^2 + y^2)$ characteristics.

Table 5 shows the possible number of trials for x that are needed. These are often less than the number of prime factors needed to establish primality. As well, additional information, that is, (*x, y*) is obtained. Another advantage is that no primes are needed for testing the primality of *N*. However, more importantly, the aim here is to establish equations that derive from integer structure and hence more accurately describe primes.

N	Row	(*x,y*)	Factors	Class of factors
57	14	-	3 ×19	$\overline{3}_4\,\overline{3}_4$
77	19	-	11×7	$\overline{3}_4\,\overline{3}_4$
117	29	(99,6)	9×13	$1_4\ 1_4$
177	44	-	3×59	$\overline{3}_4\,\overline{3}_4$
217	54	-	7×31	$\overline{3}_4\,\overline{3}_4$
237	59	-	3×79	$\overline{3}_4\,\overline{3}_4$
297	74	-	3×11	$\overline{3}_4\,\overline{3}_4$
357	89	-	3×119	$\overline{3}_4\,\overline{3}_4$
377	94	(11,16)(19,4)	13×29	$1_4\ 1_4$
417	104	-	3×139	$\overline{3}_4\,\overline{3}_4$
437	109	-	23×19	$\overline{3}_4\,\overline{3}_4$
477	119	(21,6)	3×53	$1_4\ 1_4$
497	124	-	7×71	$\overline{3}_4\,\overline{3}_4$
517	129	-	11×47	$\overline{3}_4\,\overline{3}_4$
537	134	-	3×179	$\overline{3}_4\,\overline{3}_4$
597	149	-	3×199	$\overline{3}_4\,\overline{3}_4$
637	159	-	3×53	$\overline{3}_4\,\overline{3}_4$
657	164	(9,24)	9×73	$1_4\ 1_4$
697	174	(11,24)(21,16)	17×41	$1_4\ 1_4$
717	179	-	3×239	$\overline{3}_4\,\overline{3}_4$
737	184	-	11×67	$\overline{3}_4\,\overline{3}_4$
777	194	-	3×7×37	$\overline{3}_4\,\overline{3}_4\,1_4$
817	204	-	19×43	$\overline{3}_4\,\overline{3}_4$
837	209	-	3×31	$\overline{3}_4\,\overline{3}_4$
897	224	-	3×13×23	$\overline{3}_4\,1_4\,\overline{3}_4$
917	229	-	7×131	$\overline{3}_4\,\overline{3}_4$
957	239	-	3×79	$\overline{3}_4\,\overline{3}_4$
1017	254	(21,24)	9×113	$1_4\ 1_4$
1037	259	(29,14)(19,26)	17×61	$1_4\ 1_4$
1057	264	-	7×151	$\overline{3}_4\,\overline{3}_4$
1157	289	(31,14)(1,34)	13×89	$1_4\ 1_4$

Table 3

p	Row	(x,y)	p	Row	(x,y)	p	Row	(x,y)	p	row	(x,y)
5	1	1,2	269	67	13,10	593	148	23,8	941	235	29,10
13	3	3,2	277	69	9,14	601	150	5,24	953	238	13,28
17	4	1,4	281	70	5,16	613	153	17,18	977	244	31,4
29	7	5,2	293	73	17,2	617	154	19,16	997	249	31,6
37	9	1,6	313	78	13,12	641	160	25,4	1009	252	15.28
41	10	5,4	317	79	11,14	661	165	25,6	1013	253	23,22
53	13	7,2	337	84	9,16	673	168	23,12	1021	255	11,30
61	15	5,6	349	87	5,18	677	169	1,26	1033	258	3,32
73	18	3,8	353	88	17,8	701	175	5,26	1049	262	5,32
89	22	5,8	373	93	7,18	709	177	15,22	1061	265	31,10
97	24	9,4	389	97	17,10	733	183	27,2	1069	267	13,30
101	25	1,10	397	99	19,6	757	189	9,26	1093	273	33,2
109	27	3,10	401	100	1,20	761	190	19,20	1097	274	29,16
113	28	7,8	409	102	3,20	769	192	25,12	1109	277	25,22
137	34	11,4	421	105	15,14	773	193	17,22	1117	279	29,26
149	37	7,10	433	108	17,12	797	199	11,26	1129	282	27,20
157	39	11,6	449	112	7,20	809	202	5,28	1153	288	33,8
173	43	13,2	457	114	21,4	821	205	25,14	1181	295	5,34
181	45	9,10	461	115	19,10	829	207	27,10	1193	298	13,32
193	48	7,12	509	127	5,22	853	213	23,18	1201	300	25,24
197	49	1,14	521	130	11,20	857	214	29,4	1213	303	27,22
229	57	15,2	541	135	21,10	877	219	29,6	1217	304	31,16
233	58	13,8	557	139	19,14	881	220	25,16	1229	307	35,2
241	60	15,4	569	142	13,20	929	232	23,20	1237	309	9,34
57	64	1,16	577	144	1,24	937	234	19,24	1249	312	15,32

Table 4

p	row	x, y	Number of trials of x
1277	319	11,34	1,11 (9,19,29)
1289	322	35,8	5,25,35 (3,13,23,33) (7,17,27)
1297	324	1,36	1, (9,19,29)
1301	325	25,26	5,25 (1,11,21,31) (9,19,29)
1321	330	5,36	5 (1,11,21,31) (9,19,29)
1361	340	31,20	1,11,21,31 (5,15,25,35) (9,19,29)
1373	343	37,2	7,17,27,37 (3,13,23,33)
1409	352	25,28	3,13,23,33 (5,15,25) (7,17,27,37)
1597	399	21,34	1,11,21 (9,19,29,39)
1613	403	13,38	3,13 (7,17,27,37)
1621	405	39,10	1,11,21,31 (5,15,25,35) (9,19,29,39)
1637	409	31,26	1,11,21,31 (9,19,29,39)
1657	414	19,36	9,19 (1,11,21,31)

Table 5

(iii) Characteristics of different $N*$

Only $N*$ = 1 or 7 gives $x = 1$. For this value of x the row of N must be a square since

$$4r_1 + 1 = 1 + y^2 \tag{2.2}$$

Thus $r_1 = (y/2)^2$

For $p^* = 7$, when $(y/2)^2$ is even the row of the row is also a square. When $(y/2)^2$ is odd then the row of the row = 6*K*, with

$$K = \frac{n}{2}(3n \pm 1) \tag{2.3}$$

provided $3 \nmid \frac{y}{2}$ [1]. If $3 | \frac{y}{2}$ the row of $(y/2)^2$ follows the triangular numbers.

For $p^* = 1$ and $x = 1$, $5 | r_1$. When $(y/2)^2$ is even the row of the row is square. When $(y/2)^2$ is odd the row of the row = 6*K*, as for $p^* = 7$.

For $p^* = 9$ the rows of the primes have REDs 2 or 7 hence $r_i - r_{i-1} = 5k$. Since $x^* = 5$ dominates it would be best to start with the RED, i.e. 5, 15, 25, 35,… when searching for the appropriate x.

For $p^* = 3$ the rows of the primes have REDs of 3 or 8, thus $r_i - r_{i-1} = 5k$. There is an even distribution between $x^* = 3$ and $x^* = 7$.

As an example, we shall examine the row structure for $p^* = 7$. This will indicate the sort of functions that are most appropriate for predicting primes.

3. Primes in Class $\bar{1}_4$ with a RED = 7

For these primes $x^* = 1,9$ and $y^* = 4,6$ (Table 2). With

$$x^2 = 4r_1 + 1 \tag{3.1}$$

Then $r_1 = 6K$ with

$$K = \tfrac{n}{2}(3n \pm 1) \tag{3.2}$$

provided $3 \nmid x$ [1]. When $3 | x$

$$r_1 = 2 + 18\sum_{i=1}^{j} i \tag{3.3}$$

with

$$\sum_{i=1}^{j} i = \tfrac{n}{2}(n+1) \tag{3.4}$$

Also

$$y^2 = 4r_0 \tag{3.5}$$

with r_0 being a square, that is

$$r_0 = (y/2)^2 \tag{3.6}$$

The row of r_0 (or r_1') when $(y/2)$ is odd, is given by $r_1' = 6K$ as above or, when having a factor of 3, r_1' is given by equation (3.3). When $(y/2)$ is even the row will be a square.

(i) $(y/2)$ is odd

(a) *x, y* prime to 3. With

$$x^2 = 4r_1 + 1 \tag{3.7}$$

Then $r_1 = 3n(3n \pm 1)$ and

$$y^2 = 4r_0,\ r_0 \text{ odd} \tag{3.8}$$

$$r_0 = (y/2)^2 = 4r_1' + 1 \tag{3.9}$$

with $r' = 3m(3m \pm 1)$.
Then

$$\begin{aligned} p &= x^2 + y^2 \\ &= 4r_1 + 1 + 4r_0 \\ &= 4(r_1 + r_0) + 1 \end{aligned} \tag{3.10}$$

The row of the prime, R_1, equals $(r_1 + r_0)$ thus

$$R_1 = 3n(3n \pm 1) + 12m(3m \pm 1) + 1 \tag{3.11}$$

Let $\frac{q}{2}(3q+1) \in \mathrm{I}$, $q = n, m$ and $\frac{q}{2}(3q-1) \in \mathrm{II}$, then there will be four different combinations to give the equations for rows of primes and hence the prime from $4r_1 + 1$ (Table 6).

f(*n*) category for x, y	Functions giving rows of primes	No
I.I	$9(n^2+4m^2)+3(n+4m)+1$	1
II.II	$9(n^2+4m^2)-3(n+4m)+1$	2
II.I	$9(n^2+4m^2)-3(n-4m)+1$	3
I.II	$9(n^2+4m^2)+3(n-4m)+1$	4

Table 6

It is found that *x*, *y*, *n* and *m* follow regular functions (Table 7). These are indicated in Table 8 illustrating prime production from the $f(n,m)$ in Table 6.

$f(q)$	x	n	$(y/2)$ odd	m
I	19 + 30t	3 + 5t (a)	7 + 30s	1 + 5s (e)
	31 + 30t	5 + 5t (b)	13 + 30s	2 + 5s (f)
II	11 + 30t	2 + 5t (c)	17 + 30s	3 + 5s (g)
	29 + 30t	5 + 5t (d)	23 + 30s	4 + 5s (h)

Table 7: Functions for x, y and $f(q)$ for rows of x^2 and $(y/2)^2$ (odd).

y	x	n	t	$f(t)$	m	a	$f(s)$	R_1 row of p	Prime, p, $4R_1+1=x^2+y^2$
I.I Equation 1 Table 6									
14	19	3	0	a	1	0	e	139	557
	61	10	1	b				979	3917
206	19	3	0	a	17	3	f	10699	42797
	31	5	0	b				10849	43397
	79	13	2	a				12169	48677
314	61	10	1	b	26	5	e	25579	102317
	91	15	2	b				26719	106877
	109	18	3	a				27619	110477
II.II Equation 2 Table 6									
34	11	2	0	c	3	0	g	319	1277
	41	7	1	c				709	2837
	59	10	1	d				1159	4637
	71	12	2	c				1549	6197
214	59	10	1	d	18	3	g	12319	49277
	89	15	2	d				13429	53717
	101	17	3	c				13999	55997
346	29	5	0	d	29	5	h	30139	120557
	89	15	2	d				31909	127637
	101	17	3	c				32479	129917
II.I Equation 3 Table 6									
26	11	2	0	c	2	0	f	199	797
	41	7	1	c				589	2357
	59	10	1	d				1039	4157
	71	12	2	c				1429	5717
	89	15	2	d				2149	8597
326	11	2	0	c	27	5	f	26599	106397
	71	12	2	c				27829	111317
	89	15	2	d				28549	114197
I.II Equation 4 Table 6									
34	31	5	0	b	3	0	g	529	2117
	49	8	1	a				889	3557
	61	10	1	b				1219	4877
	91	15	2	b				2359	9437
	109	18	3	a				3259	13037
346	19	3	0	a	29	5	h	30019	120077
	31	5	0	b				30169	120667
	49	8	1	a				30529	122117
	91	15	2	b				31999	127997

Table 8

(b) *x* or *y* with a factor of 3

When $3 \nmid x, r_1 = 3n(3n \pm 1)$ as before, but when $3|y$, r' for r_0 or (y/2) is given by Equation (3.3). Some examples are given in Table 9.
Thus the equations for the rows of the primes are:

$$R_1 = 9\left(n^2 + 4m^2\right) + 3\left(n + 12m\right) + 9, \qquad Ia, \tag{3.12}$$

or

$$R_1 = 9\left(n^2 + 4m^2\right) - 3\left(n - 12m\right) + 9, \qquad IIa. \tag{3.13}$$

$(y/2)$	**Row of** $(y/2)^2$	**m**	93	2162	15
3	2	0	117	3422	19
27	182	4	123	3782	20
33	272	5	147	5402	24
57	812	9	153	5852	25
63	992	10	177	7832	29
87	1892	14→↑	183	8372	30

Table 9

Examples using these equations are listed in Table 10.

x	***y***	**Row of** x^2	**Row of** $(y/2)^2$	***n***	**Eq**	***m***	**Row of *p***	**Prime, *p***
11	6	30	2	2	II	0	39	157
19		90	2	3	I	0	99	397
29		210	2	5	II	0	219	877
31		240	2	5	I	0	249	997
91		2070	2	15	I	0	2079	8317
11	234	30	3422	2	II	19	13719	54877
19		90	3422	3	I	19	13779	55117
31		240	3422	5	I	19	13929	55717
41		420	3422	7	II	19	14109	56437
59		870	3422	10	II	19	14559	58237
61		930	3422	10	I	19	14619	58477
71		1260	3422	12	I	19	14949	59797

Table 10

When $3|x$ we get

$$r_1 = 2 + 18\left(\tfrac{1}{2}n\left(n+1\right)\right) \tag{3.14}$$
$$r_0 = 4r_1' + 1$$

with

$$r' = 3m(3m \pm 1), \tag{3.15}$$

so row of prime, R_1, is given by

$$R_1 = 9\left(n^2 + 4m^2\right) + 3(3n + 4m) + 3, \;\; m \in I, \tag{3.16}$$

or

$$R_1 = 9\left(n^2 + 4m^2\right) + 3(3n - 4m) + 3, \;\; m \in II. \tag{3.17}$$

For example, let $x = 9$, $y = 14$, then $r_1 = 20$, $n = 1$ and row = 49, $r' = 6\times 2$, $m = 1$ (I) so that row of prime = 69 and prime = 277.

(ii) $(y/2)$ **is even**

In general, $(y/2)^2 = r_0$ and $(y/2) = 2^q t$ where t is a positive odd integer.
When q = 0, then y/2 will be odd, so that $r_0 = t^2$ (Section 3(i).)
Here q > 0 and

$$r_0 = 2^{2q} t^2. \tag{3.18}$$

(a) $t > 1$ **and** $3 \nmid t, x.$

The same form of equation as above will also apply here, that is with prime $p \in \bar{1}_4$

$$p = 4r_1 + 1 = x^2 + y^2 \tag{3.19}$$

with $x^2 = 4r_1' + 1$ and $y^2 = 4r_0$ so that

$$p = 4(r_1' + r_0) + 1. \tag{3.20}$$

Then the row of the prime equals $(r_1' + r_0)$ as before.
Since

$$r' = 6K = 3n(3n \pm 1) \tag{3.21}$$

and r_0 is represented by

$$\begin{aligned} r_0 &= 2^{2q} t^2 \\ &= 2^{2q}(4r_1'' + 1) \end{aligned} \tag{3.22}$$

with $r_1'' = 3m(3m \pm 1)$, the row of the prime becomes

$$r_1' + r_0 = 3n(3n \pm 1) + 2^{2q}(12m(3m \pm 1) + 1). \tag{3.23}$$

Some examples are given in Table 11.

***y*/2**	***q***	***t***	r_1''	***K***	***m***	***n* for various *x****	**Row of *p***	***p***
22	1	11	30	5	211	I 3,<u>5</u>,7,8,10	724	2897
						II 5,10,12,15		
52	2	13	42	7	21	I 3,5,7,8,10	2734	10937
						II <u>2</u>,5		
62	1	31	240	40	51	I 3,13	6394	25577
						II 2,5,15,<u>17</u>		
82	1	41	420	70	711	I <u>8</u>	7324	29297
						II 2,5,17		
92	2	23	132	22	411	I 3,7,<u>18</u>	11434	45737
						II 10,15		

Table 11: * underlined value used for *p*

(b) ***x*** **or** ***y*** **with factor of 3**

The development is similar to that in Section 3 (i) (b), except that

$$r_0 = 2^{2q} f(m). \tag{3.24}$$

(c) $t = 1$

The row of the prime is simply given by

$$R_1 = r_1' + r_0 = 3n(3n \pm 1) + 2^{2q}. \qquad (3.25)$$

For example, with $y/2$ = 128, r_0 = 16384, q = 7, and with x = 79, x^2 = 6241 with a row = 6×260 so that n = 131. Some other suitable x are 11, 29, 41, 61, 109.

4. Final Comments

Integer structure analysis shows that primes $\in \bar{1}_4$ have the form $4R_1 + 1$ where $R_1 = r_1 + r_0$ from $x^2 = 4r_1 + 1$ and $y^2 = 4r_0$ with $r_1 = 3n(3n \pm 1)$, or if $3 \mid x$, $r_1 = 2 + 9n'(n' + 1)$, and

$$r_0 = 2^{2q}\left(12m(3m \pm 1) + 1\right),$$

or if $3 \mid y$,

$$r_0 = 2^{2q}\left(4\left(2 + 9m'(m'+1)\right) + 1\right).$$

When q = 0, $y/2$ is odd, and m = 0 yields $r_0 = 2^{2q}$. Primes with a RED of 7 have been used as an example here but the same equations can be applied to all primes in Class $\bar{1}_4$. A similar analysis may be made for primes in Class $\bar{3}_4$ but in this case

$$p = y^2 - x^2 \qquad (4.1)$$

with $y - x = 1$ and $(y, x) \in \{(\bar{0}_4, \bar{3}_4), (\bar{2}_4, \bar{1}_4)\}$. Since the squares follow $f(n)$ and $f(m)$, similar equations arise. When $n = m$, the equations have the form

$$f(n) = An^2 + Bn + C \qquad (4.2)$$

which is similar to Euler's prime generating equation, and the recently developed prime equations for the modular ring Z_6 [1, 2, 3].

References

[1] Leyendekkers, J.V., A.G. Shannon, J.M. Rybak. 2007. *Pattern Recognition: Modular Rings and Integer Structure*. North Sydney: Raffles KvB Monograph No 9.

[2] Leyendekkers, J.V., A.G. Shannon. 2008. Analysis of Primes Using Right-end-digits and Integer Structure. *Notes on Number Theory and Discrete Mathematics.* 14(3): 1-10.

[3] Leyendekkers, J.V., A.G. Shannon. 2008. The identification of Rows of Primes in the Modular Ring Z_6. *Notes on Number Theory and Discrete Mathematics.* 14(3): 10-16.