Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 21, 2015, No. 4, 17–21

The sum of squares for primes

J. V. Leyendekkers[1] and A. G. Shannon[2,3]

[1] Faculty of Science, The University of Sydney, NSW 2006, Australia
[2] Faculty of Engineering & IT, University of Technology, Sydney, NSW 2007, Australia
[3] Campion College, PO Box 3052, Toongabbie East, NSW 2146, Australia
e-mails: t.shannon@campion.edu.au,
Anthony.Shannon@uts.edu.au

Abstract: Only prime integers that are in Class $\bar{1}_4$ of the Modular Ring Z_4 equate to a sum of squares of integers x and y. A simple equation to predict these integers is developed which distinguishes prime and composite numbers in that one (x, y) couple exists for primes, but composites have either one couple with a common factor or the same number of couples as there are factors. In particular, composite Fibonacci numbers always have multiple (x, y) couples because the factors are all elements of $\bar{1}_4$.
Keywords: Modular rings, Fibonacci sequence, Prime numbers, Composite numbers, Right-end-digits, Pascal-Fibonacci numbers.
AMS Classification: 11B39, 11B50.

1 Introduction

Fermat showed that odd integers which equal a sum of squares have the form $4r + 1$, which is obvious in the modular ring Z_4 [6] (Table 1). If we consider $N = x^2 + y^2$ with x odd and y even, then we see that odd squares are elements of class $\bar{1}_4$ and even squares are elements of $\bar{0}_4$ only.

Row $r_i \downarrow$ / **Class** $i \rightarrow$	$\bar{\mathbf{0}}_4$	$\bar{\mathbf{1}}_4$	$\bar{\mathbf{2}}_4$	$\bar{\mathbf{3}}_4$	**Comments**
0	0	1	2	3	$N = 4r_i + i$
1	4	5	6	7	even $\bar{0}_4$, $\bar{2}_4$
2	8	9	10	11	$\left(N^n, N^{2n}\right) \in \bar{0}_4$
3	12	13	14	15	odd $\bar{1}_4, \bar{3}_4$; $N^{2n} \in \bar{1}_4$

Table 1. Classes and rows for Z_4

We then have the two possibilities

$$\bar{1}_4 + \bar{0}_4 \begin{cases} = \bar{1}_4, & N \in \bar{1}_4 \Rightarrow N \text{ can be a sum of squares}, \\ \neq \bar{3}_4, & N \in \bar{3}_4 \Rightarrow N \text{ cannot be a sum of squares}; \end{cases} \tag{1.1}$$

that is, only prime numbers which are elements of $\bar{1}_4$ can be a sum of squares. In this note we develop a means of calculating *x* and *y* rapidly in the sense of experimental mathematics [1].

2 Calculations

Thus for $p \in \bar{1}_4$,

$$p = x^2 + y^2 = (x + y)^2 - 2xy. \tag{2.1}$$

If $A = x + y$, then

$$x, y = \frac{A \pm \sqrt{2p - A^2}}{2} \tag{2.2}$$

which gives an upper limit of $\sqrt{2p}$ for *A*. *x* (odd) and *y* (even) are the two solutions of (2.2). We now show that $(2p - A^2)^* \in \{1, 5, 9\}$.

The primes, *p*, can be divided into four types according, p^*, to their right-end-digits (REDs) [*cf.* 8]; that is, according to their classes in the modular ring Z_5 [2, 6]. $p^* \in \{1, 3, 7, 9\}$ corresponding to classes $\bar{1}_5, \bar{3}_5, \bar{2}_5, \bar{4}_5$ so that the class of *A** in Z_5 will be determined by p^*, but odd squares only have REDs equal to 1,5,9 (Table 2).

p^*	A^*	A^{2*}
1	1, 9	1
3	1, 5, 9	1, 5
7	3, 5, 7	5, 9
9	3, 7	9

Table 2. Restraints on REDs

3 Examples of *x*, *y* in $\bar{1}_4$

In the spirit of Phillips [9], samples of primes with calculated *A*, *x* and *y* are displayed in Tables 3, 4, 5, 6.

p	*A*	$\sqrt{2p}$	*x*	*y*	*p*	*A*	$\sqrt{2p}$	*x*	*y*
41	9	9.1	5	4	941	39	43.4	29	10
101	11	14.2	1	10	1061	41	46.1	31	10
241	19	22.0	15	4	1201	49	49.0	25	24
401	21	28.3	1	20	1381	49	52.5	15	34
541	31	32.9	21	10	1621	49	56.9	39	10
661	31	36.4	25	6	1741	59	59.0	29	30
761	39	39.0	19	20	113341	461	476.0	171	290
821	39	40.5	25	14	530861	1011	1030.4	605	406

Table 3. $p^* = 1$, $A^* = 1, 9$

p	A	$\sqrt{2p}$	x	y	p	A	$\sqrt{2p}$	x	y
13	5	5.1	3	2	853	41	41.3	23	18
113	15	15.0	7	8	1013	45	45.0	23	22
233	21	21.6	13	8	1153	41	48.0	33	8
313	25	25.0	13	12	1213	49	49.3	27	22
433	29	29.4	17	12	1453	41	53.9	3	38
593	31	34.4	23	8	1613	51	56.8	13	38
673	35	36.7	23	12	1733	55	58.9	17	38
733	29	38.3	27	2	113153	459	475.7	167	292

Table 4. $p^* = 3$, $A^* = 1, 5, 9$

p	A	$\sqrt{2p}$	x	y	p	A	$\sqrt{2p}$	x	y
17	5	5.8	1	4	977	35	44.2	31	4
137	15	16.6	11	4	1097	45	46.8	29	16
257	17	22.7	1	16	1217	47	49.3	31	16
317	25	25.2	11	14	1297	37	50.9	1	36
397	25	28.2	19	6	1597	55	56.5	21	34
557	33	33.4	19	14	1657	55	57.6	19	36
677	27	36.8	1	26	113497	475	476.0	219	256
857	33	41.4	29	4	113777	477	477.0	241	236

Table 5. $p^* = 7$, $A^* = 3, 5, 7$

p	A	$\sqrt{2p}$	x	y	p	A	$\sqrt{2p}$	x	y
29	7	7.6	5	2	809	33	40.2	5	28
89	13	13.3	5	8	929	43	43.1	23	20
149	17	17.3	7	10	1069	43	46.2	13	30
269	23	23.2	13	10	3329	77	81.6	25	52
389	27	27.9	17	10	7489	113	122.4	33	80
449	27	30.0	7	20	7589	123	123.2	65	58
569	33	33.7	13	20	7669	97	123.8	87	10
709	37	37.7	15	22	113209	403	475.8	75	328
					534629	1017	1034.0	415	602

Table 6. $p^* = 9$, $A^* = 3, 7$

4 Fibonacci primes

The x, y values for Fibonacci primes, F_p, are obtained simply from [7]

$$F_p = F^2_{\frac{p+1}{2}} + F^2_{\frac{p-1}{2}} \tag{4.1}$$

in which

$$F_p = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p\right), \tag{4.2}$$

the Binet equation [7], or from the Pascal-Fibonacci equation [3, 4]

$$F_p = 2 + \sum_{i=2}^{\frac{p-1}{2}} \binom{p-i}{i-1} \tag{4.3}$$

from which the individual Pascal-Fibonacci (PF) numbers, N_n, can be given by

$$N_p = \binom{p-i}{i-1}. \tag{4.4}$$

For example, for $p = 17$, $F_p = 1597$, and the Binet and Pascal-Fibonacci equations (4.2) and (4.3) then yield respectively

$$F_{17} = \begin{cases} \dfrac{1}{\sqrt{5}}\left(\left(\dfrac{1+\sqrt{5}}{2}\right)^{17} - \left(\dfrac{1-\sqrt{5}}{2}\right)^{17}\right) & = 1597, \\ 2 + 15 + 91 + 286 + 495 + 462 + 210 + 36 & = 1597. \end{cases}$$

From (2.2) and (4.1) we get

$$A = F_{\frac{p+1}{2}} + F_{\frac{p-1}{2}}. \tag{4.5}$$

For example, if $p = 11$, then $F_{11} = 89 = F_6^2 + F_5^2 = 25 + 64$. That is, $A = 13$ so that $x = \frac{1}{2}\left(13 - \sqrt{178 - 169}\right) = 5$ and $y = \frac{1}{2}(13 + 3) = 8$, as required (Table 6).

5 Composites as sums of squares

As with prime integers, only odd composite integers in class $\bar{1}_4$ can equal a sum of squares [6], but the number of (x, y) ordered pairs will be the same as the number of prime factors.

N	***Factors***	***Classes***	***A***	$\sqrt{2p}$	***x***	***y***
57	3×19	$\bar{3}_4\bar{3}_4$	–	10.7	–	–
117	$3 \times 3 \times 13$	$\bar{3}_4\bar{3}_4\bar{1}_4$	15	15.29	3×3	3×2
177	3×59	$\bar{3}_4\bar{3}_4$	–	18.8	–	–
217	7×31	$\bar{3}_4\bar{3}_4$	–	20.8	–	–
297	$3 \times 3 \times 3 \times 11$	$\bar{3}_4\bar{3}_4\bar{3}_4\bar{3}_4$	–	24.4	–	–
357	$3 \times 7 \times 17$	$\bar{3}_4\bar{3}_4\bar{1}_4$	–	26.7	–	–
377	13×29	$\bar{1}_4\bar{1}_4$	27	27.5	11	16
			23		19	4
417	3×139	$\bar{3}_4\bar{3}_4$	–	28.9	–	–
437	19×23	$\bar{3}_4\bar{3}_4$	–	29.6	–	–
477	$3 \times 3 \times 53$	$\bar{3}_4\bar{3}_4\bar{1}_4$	27	30.9	3×7	3×2
497	7×71	$\bar{3}_4\bar{3}_4$	–	31.5	–	–

Table 7. $p^* = 7$; $A^* = 3, 5, 7$

If the factors all come from class $\bar{3}_4$, then there will be no sum of squares, but if some factors come from class $\bar{1}_4$, then there can be a sum of squares [6]. In some cases there is only

one ordered pair but, unlike the primes, x and y have a common factor in this case. Some examples are displayed in Table 7 for $p^* = 7$. Similar results may be found for $p^* = 1$, 3 or 9.

Note that 1517 (11 × 47), 537 (3 × 179) and 597 (3 × 199) all have factors in $\bar{3}_4$ only, so there are no sums of squares.

For composite Fibonacci numbers with prime subscripts there are as many ordered pairs (x, y) as there are factors. For example,

- F_{31} = 1, 346, 269 has 2 factors, $557 \in \bar{1}_4, 2417 \in \bar{1}_4$, and 2 (x, y) ordered pairs: (987, 610) and (875, 762);
- F_{37} = 24, 157, 817 has 3 factors, all in class $\bar{1}_4$, and thus 3 (x,y) ordered pairs: (4181, 2584), (4909, 224) and (3859, 3044).

For all the F_p values identified as composite (F_{19} to F_{97}) the factors are all in class $\bar{1}_4$ [5] so that there are multiple (x,y) ordered pairs for these integers [3].

6 Composites as sums of squares

These distinct differences between prime and composite numbers in class $\bar{1}_4$ is useful for primality testing in that class, particularly as the integers increase in value the number of steps needed to find A do not necessarily increase. For instance, for $p^* = 9$ (Table 6), $p = 7589$ takes only one step while $p = 7669$ takes six steps, whereas for $p = 534629$, only four steps are need to obtain A.

References

[1] Borwein, J, & D. Bailey. (2004) *Mathematics by Experiment: Plausible Reasoning in the 21st Century*. Natick, MA: A K Peters.

[2] Leyendekkers, J. V. & A. G. Shannon (2012) The Modular Ring Z_5. *Notes on Number Theory and Discrete Mathematics.* 18(2), 28–33.

[3] Leyendekkers, J. V. & A. G. Shannon (2013) Fibonacci and Lucas Primes. *Notes on Number Theory and Discrete Mathematics.* 19(2), 49–59.

[4] Leyendekkers, J. V. & A. G. Shannon (2013) The Pascal-Fibonacci Numbers. *Notes on Number Theory and Discrete Mathematics.* 19(3), 5–11.

[5] Leyendekkers, J. V. & A. G. Shannon (2014) Fibonacci Primes. *Notes on Number Theory and Discrete Mathematics.* 20(2), 6–9.

[6] Leyendekkers, J. V., A. G. Shannon, & J. M. Rybak (2007) *Pattern Recognition: Modular Rings and Integer Structure.* North Sydney: Raffles KvB Monograph No. 2.

[7] Livio, M. (2002) *The Golden Ratio.* New York: Golden Books.

[8] Omey, E., S. Van Gulck. (2015) What are the last digits of ... ? *International Journal of Mathematical Education in Science and Technology*. 46(1), 147–155.

[9] Phillips, G. M. (2005) *Mathematics is not a Spectator Sport.* New York: Springer.