お茶の水女子大学自然科学報告　第58巻　第1号
Natural Science Report, Ochanomizu University, Vol. 58, No. 1 (2007)

Pell Equation. IV. Fastest algorithm for solving the Pell equation

Haruo Hosoya

(Received April 10, 2007)

Abstract The fastest algorithm for solving the Pell equations, $x^2 - D y^2 = 1$ (called Pell-1) and $x^2 - D y^2 = -1$ (Llep-1), are demonstrated with two typical examples. The essence of the algorithm is i) to obtain the periodic continued fraction expression for the square root of D, ii) to prepare four caterpillar graphs by using the terms derived above, and iii) to set a 3×3 (for Pell) or 2×2 (for Llep) determinant whose elements are the topological indices (Z's) of those graphs, and iv) to calculate the determinant. The dramatic shortening of the procedure comes from the finding that the continuant is equivalent to the topological index of the caterpillar graph directly derived from the continued fraction expansion of the square root of D.

1. Introduction

Let us call Eqns. (1.1) and (1.2), respectively, Pell-1 and Llep-1,[1-4]

$$x^2 - D y^2 = 1 \qquad \text{(Pell-1)} \tag{1.1}$$

$$r^2 - D s^2 = -1, \qquad \text{(Llep-1)} \tag{1.2}$$

where only natural number solutions (x, y) are to be sought for square-free natural number D.[1-7] It is known that for any D (1.1) is solvable, whereas for a limited number of D's (1.2) has solutions. For Llep-1 to be solvable at least D is the sum of a pair of squares, but this is not the necessary condition. Anyway once the smallest solution (r_1, s_1) of (1.2) is obtained, all other families of not only (1.2) but also (1.1) with the same D can be obtained from it. In that case we call the combined equations of (1.1) and (1.2) "Pellep-1",[1-4] namely,

$$t^2 - D u^2 = \pm 1. \qquad \text{(Pellep-1)} \tag{1.3}$$

According to the standard recipe developed by Lagrange simple continued fractions, either finite or infinite periodic, are known to play a key role in solving the Pell equations, (1.1)-(1.3).[5-7] For degrading a given continued fraction the so-called "continuants" were proposed by Euler.[7-10] It was recently found[11] that instead of following iterative steps for this degradation, 600 years before the work of these European mathematical giants, Bhaskara II in old India found more efficient jumping algorithm for reaching the final result.

In the former paper[4] of the present series the present author has shown that the continuant is identical to the topological index Z,[12,13] of a caterpillar graph[14,15] composed solely of the terms of the continued fraction concerned. Further by using the graph-theoretical technique developed by the present author the smallest solution of the Pell equations can be represented by a 2×2 or 3×3 determinant whose elements are the Z-indices of certain subgraphs of the caterpillar.

In this paper, after introducing the proposed algorithm examples for solving the Pell equations will be demonstrated and discussed.

2. Algorithm

First obtain the continued fraction expansion of the square root of D. However, depending on the parity of the length k of the period of the infinite continued fractions the necessary procedures are a little different from each other.

2. 2 Pell-1 with even $k=2m$

$$\begin{aligned}\sqrt{D} &= [a_0;\overline{a_1,a_2,\cdots,a_{m-1},a_m,a_{m+1},\cdots,a_{2m-1},a_{2m}}] \\ &= [a_0;\overline{a_1,a_2,\cdots,a_{m-1},a_m,a_{m-1},a_{m-2},\cdots,a_1,2a_0}] \\ &= [a\overline{\mathrm{L}c\mathrm{L}^{-}b}] = [a\overline{\mathrm{A}b}],\end{aligned} \qquad (2.1)$$

where a, b, and c are, respectively, a_0, a_{2m}, and a_m, and L and L^{-} are, respectively, the caterpillar $\mathrm{C}_{m-1}(a_1, a_2,\cdots, a_{m-1})$ and its reversed image $\mathrm{C}_{m-1}(a_{m-1},\cdots, a_2, a_1)$. As shown in Fig. 1 a caterpillar is constructed from the path graph S_n with n vertices and the set of n star graphs, each of which (a_n=K_{1,a_n-1}) is composed of the central vertex and n–1 edges of unit length emanating from the central vertex. The above two caterpillars are denoted, respectively, as L and L^{-}, which, however, are essentially identical to each other, as they are graphs. The symbol A denotes the caterpillar $\mathrm{L}c\mathrm{L}^{-}$ with symmetrical structure beginning from and ending at the moiety of star a_1.

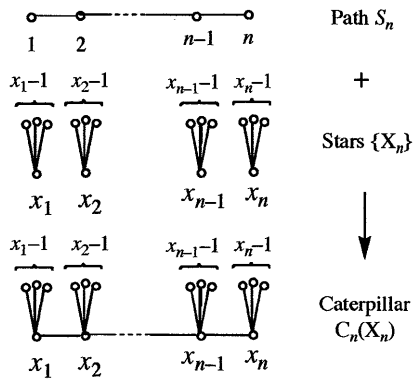


Fig. 1. A caterpillar is constructed from a path and the set of stars.

The smallest solution (x_1, y_1) of (1.1) is known to be expressed by the Z-indices of a pair of caterpillars, $\mathrm{C}_{2m-1}(\mathrm{A})$ and $\mathrm{C}_{2m}(a\mathrm{A})$, and all their family members can also be obtained as

$$x_1 = Z_{2m}(a\mathrm{A}), \quad x_2 = Z_{4m}(a\mathrm{A}b\mathrm{A}), \quad x_3 = Z_{6m}(a\mathrm{A}b\mathrm{A}b\mathrm{A}), \quad \text{etc.} \qquad (2.2)$$

$$y_1 = Z_{2m-1}(\mathrm{A}), \quad y_2 = Z_{4m-1}(\mathrm{A}b\mathrm{A}), \quad y_3 = Z_{6m-1}(\mathrm{A}b\mathrm{A}b\mathrm{A}), \quad \text{etc.} \qquad (2.3)$$

[Theorem 1] Smallest solution of Pell-1 with even k.

$$x_1 = Z_{2m}(aA) = Z_{2m}(aLcL^-) = \begin{vmatrix} aL & aM & 0 \\ -1 & c & 1 \\ 0 & -M & L \end{vmatrix} = \begin{vmatrix} Z_m(aL) & Z_{m-1}(aM) & 0 \\ -1 & a_m & 1 \\ 0 & -Z_{m-2}(M) & Z_{m-1}(L) \end{vmatrix} \tag{2.4}$$

$$y_1 = Z_{2m-1}(A) = Z_{2m-1}(LcL^-) = \begin{vmatrix} L & M & 0 \\ -1 & c & 1 \\ 0 & -M & L \end{vmatrix} = \begin{vmatrix} Z_{m-1}(L) & Z_{m-2}(M) & 0 \\ -1 & a_m & 1 \\ 0 & -Z_{m-2}(M) & Z_{m-1}(L) \end{vmatrix}. \tag{2.5}$$

Higher family members f_{n-1}'s of the solutions can be obtained by using the recursion formula[2,3]

$$f_n = 2x_1 f_{n-1} - f_{n-2}. \quad (f = x, y). \tag{2.6}$$

2.2 Llep-1 with odd $k=2m-1$

$$\begin{aligned} \sqrt{D} &= [a_0; \overline{a_1, a_2, \cdots, a_{m-1}, a_m, \cdots, a_{2m-2}, a_{2m-1}}] \\ &= [a_0; \overline{a_1, a_2, \cdots, a_{m-1}, a_{m-1}, a_{m-2}, \cdots, a_1, 2a_0}] \\ &= [a\overline{LL^- b}] = [a\overline{Ab}]. \end{aligned} \tag{2.7}$$

Note that in this case the symmetrical caterpillar $A=LL^-$ is different from case **2.1**, and has an even number of star moieties. In this case the smallest solution $(r_1, s_1) = (t_1, u_1)$ of Llep-1 (1.2) is followed by the smallest solution $(x_1, y_1) = (t_2, u_2)$ of Pell-1 (1.1), and then alternately Llep-1 and Pell-1 appear to form the big family of Pellep-1.

$$t_1 = r_1 = Z_{2m-1}(aA), \quad t_2 = x_1 = Z_{4m-2}(aAbA), \quad t_3 = r_2 = Z_{6m-3}(aAbAbA), \quad \text{etc.} \tag{2.8}$$

$$u_1 = s_1 = Z_{2m-2}(A), \quad u_2 = y_1 = Z_{4m-3}(AbA), \quad u_3 = s_2 = Z_{6m-4}(AbAbA), \quad \text{etc.} \tag{2.9}$$

Further, it was proved that once (r_1, s_1) is obtained, the larger members of Pellep-1 can also be obtained by using the Chebyshev polynomials of the second kind.[2] Especially for (t_2, u_2) we have

$$\begin{aligned} t_2 &= 2r_1^2 + 1, \\ u_2 &= 2 r_1 s_1. \end{aligned} \tag{2.10}$$

Thus the following theorem can be obtained.

[Theorem 2] Smallest solution of Llep-1 with odd k.

$$r_1 = t_1 = Z_{2m-1}(aA) = Z_{2m-1}(aLL^-) = \begin{vmatrix} aL & aM \\ -M & L \end{vmatrix} = \begin{vmatrix} Z_m(aL) & Z_{m-1}(aM) \\ -Z_{m-2}(M) & Z_{m-1}(L) \end{vmatrix} \tag{2.11}$$

$$s_1 = u_1 = Z_{2m-2}(A) = Z_{2m-2}(LL^-) = \begin{vmatrix} L & M \\ -M & L \end{vmatrix} = \begin{vmatrix} Z_{m-1}(L) & Z_{m-2}(M) \\ -Z_{m-2}(M) & Z_{m-1}(L) \end{vmatrix}. \tag{2.12}$$

The smallest solution of Pell-1 with odd k is obtained by (2.8) and (2.9). Higher family members f_{n-1}'s can be obtained by using the different recursion formula[2]

$$f_n = 2x_1 f_{n-1} + f_{n-2} \quad (f = t, u). \tag{2.13}$$

3. Worked-out examples

3. 1 Pell-1 with even k

Let us first choose D=67. Its continued fraction expansion is obtained to be

$$\sqrt{67} = [8;\overline{5,2,1,1,7,1,1,2,5,16}] \tag{3.1}$$

with its length of period, k=10. The procedure for obtaining these terms has to be given here, because one cannot skip any of the following steps for further manipulation.

$$\begin{aligned}
n=0 \quad & \sqrt{67} = 8+(\sqrt{67}-8)\\
1 \quad & \frac{1}{\sqrt{67}-8} = \frac{\sqrt{67}+8}{3} = 5+\frac{\sqrt{67}-7}{3}\\
2 \quad & \frac{3}{\sqrt{67}-7} = \frac{\sqrt{67}+7}{6} = 2+\frac{\sqrt{67}-5}{6}\\
3 \quad & \frac{6}{\sqrt{67}-5} = \frac{\sqrt{67}+5}{7} = 1+\frac{\sqrt{67}-2}{7}\\
4 \quad & \frac{7}{\sqrt{67}-2} = \frac{\sqrt{67}+2}{9} = 1+\frac{\sqrt{67}-7}{9}\\
5 \quad & \frac{9}{\sqrt{67}-7} = \frac{\sqrt{67}+7}{2} = 7+\frac{\sqrt{67}-7}{2}\\
6 \quad & \frac{2}{\sqrt{67}-7} = \frac{\sqrt{67}+7}{9} = 1+\frac{\sqrt{67}-2}{9}\\
7 \quad & \frac{9}{\sqrt{67}-2} = \frac{\sqrt{67}+2}{7} = 1+\frac{\sqrt{67}-5}{7}\\
8 \quad & \frac{7}{\sqrt{67}-5} = \frac{\sqrt{67}+5}{6} = 2+\frac{\sqrt{67}-7}{6}\\
9 \quad & \frac{6}{\sqrt{67}-7} = \frac{\sqrt{67}+7}{3} = 5+\frac{\sqrt{67}-8}{3}\\
10 \quad & \frac{3}{\sqrt{67}-8} = \sqrt{67}+8 = 16+(\sqrt{67}-8)
\end{aligned}$$

Then as shown in Fig. 2, construct caterpillar A = C_9(5, 2, 1, 1, 7, 1, 1, 2, 5) from which four subgraphs are derived. Their Z-indices can be obtained quite easily by using the following recursion formula,

$$Z(G) = Z(G-I) + Z(G\Theta I)\ , \tag{3.2}$$

where G–I is the subgraph obtained from G by deleting an arbitrary edge I, and GΘI is obtained from G–I by deleting all the edges which *were* incident to I in G.

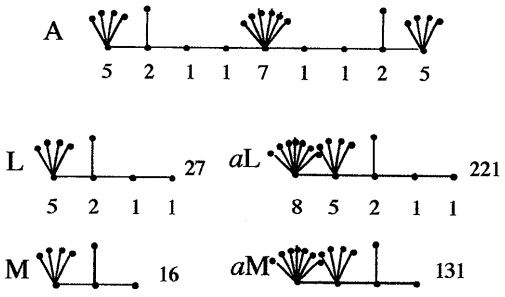


Fig. 2. The key caterpillars and their Z-values for D=67.

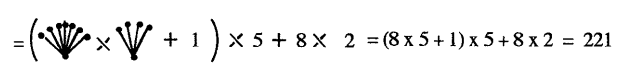
Then the resultant determinant to be solved is as follows:

$$x_1 = \begin{vmatrix} 221 & 131 & 0 \\ -1 & 7 & 1 \\ 0 & -16 & 27 \end{vmatrix} = 221\times 7\times 27 + 221\times 16 + 131\times 27 = 48842,$$

$$y_1 = \begin{vmatrix} 27 & 16 & 0 \\ -1 & 7 & 1 \\ 0 & -16 & 27 \end{vmatrix} = 27^2\times 7 + 2\times 27\times 16 = 5967.$$

Actually we have $48842^2 - 67\times 5967^2 = 1$.

It is not a difficult task to calculate the Z-index of a given caterpillar. For example, the largest one in this case aL can be obtained by the repeated use of the recursive formula (2.15) as below.



It is to be remembered that the Z-index of a path graph S_n composed of n vertices is equal to the Fibonacci number as shown below.

n	0	1	2	3	4	5	6	7	8	9	10
F_n	1	1	2	3	5	8	13	21	34	55	89.

Note, however, that the initial conditions are a little different from the conventional ones.[3,4,16,17]

Here caterpillar aL is cut at edge l marked with the double bar to yield G–l and further cut at the dotted curve to yield G⊖l. However, in the above diagram the isolated vertices are omitted, as their Z-values are all unity

3. 2 Llep-1 with odd k

Next choose D=61. Its continued fraction expansion is obtained to be

$$\sqrt{61} = [7;\overline{1,4,3,1,2,2,1,3,4,1,14}] \tag{3.3}$$

with its length of period, k=11. The above terms of the continued fraction is obtained in the following steps:

$n=0$ $\sqrt{61} = 7 + (\sqrt{61} - 7)$

1 $\dfrac{1}{\sqrt{61}-7} = \dfrac{\sqrt{61}+7}{12} = 1 + \dfrac{\sqrt{61}-5}{12}$

2 $\dfrac{12}{\sqrt{61}-5} = \dfrac{\sqrt{61}+5}{3} = 4 + \dfrac{\sqrt{61}-7}{3}$

3 $\dfrac{3}{\sqrt{61}-7} = \dfrac{\sqrt{61}+7}{4} = 3 + \dfrac{\sqrt{61}-5}{4}$

4 $\dfrac{4}{\sqrt{61}-5} = \dfrac{\sqrt{61}+5}{9} = 1 + \dfrac{\sqrt{61}-4}{9}$

5 $\dfrac{9}{\sqrt{61}-4} = \dfrac{\sqrt{61}+4}{5} = 2 + \dfrac{\sqrt{61}-6}{5}$

6 $\dfrac{5}{\sqrt{61}-6} = \dfrac{\sqrt{61}+6}{5} = 2 + \dfrac{\sqrt{61}-4}{5}$

7 $\dfrac{5}{\sqrt{61}-4} = \dfrac{\sqrt{61}+4}{9} = 1 + \dfrac{\sqrt{61}-5}{9}$

8 $\dfrac{9}{\sqrt{61}-5} = \dfrac{\sqrt{61}+5}{4} = 3 + \dfrac{\sqrt{61}-7}{4}$

9 $\dfrac{4}{\sqrt{61}-7} = \dfrac{\sqrt{61}+7}{3} = 4 + \dfrac{\sqrt{61}-5}{3}$

10 $\dfrac{3}{\sqrt{61}-5} = \dfrac{\sqrt{61}+5}{12} = 1 + \dfrac{\sqrt{61}-7}{12}$

11 $\dfrac{12}{\sqrt{61}-7} = \sqrt{61}+7 = 14 + (\sqrt{61}-7)$

Then construct caterpillar C_{10}(1, 4, 3, 1, 2, 2, 1, 3, 4, 1) from which four subgraphs are derived as shown in Fig. 3.

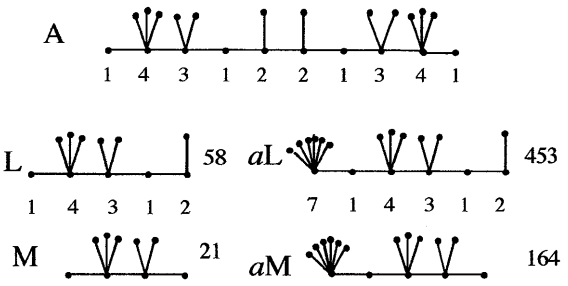


Fig. 3. The key caterpillars and their Z-values for D=61.

Then the resultant determinant to be solved is as follows:

$$t_1 = r_1 = \begin{vmatrix} 453 & 164 \\ -21 & 58 \end{vmatrix} = 453 \times 58 + 164 \times 21 = 29718,$$

$$u_1 = s_1 = \begin{vmatrix} 58 & 21 \\ -21 & 58 \end{vmatrix} = 58^2 + 21^2 = 3805.$$

Actually we have $29718^2 - 61 \times 3805^2 = -1$, which is the smallest solution of Llep-1. The famous smallest solution of Pell-1 for D=61 can be obtained as follow:

$$t_2 = x_1 = 2 \times 29718^2 + 1 = 1766319049,$$

$$u_2 = y_1 = 2 \times 29718 \times 3805 = 226153980.$$

4. Comparison with the conventional algorithm

Let us compare the present algorithm with the widely known one originally proposed by Lagrange. Although there are several modified versions, here we take the one in which the terms of the continued fractions are obtained first. Then all the set of a_n's are already given in Table 1. After setting $p_{-1}=1$, $p_0=a_0$, $q_{-1}=0$, and $q_0=1$, we proceed according to the following recursive steps

$$p_n = a_n p_{n-1} + p_{n-2},$$

$$q_n = a_n q_{n-1} + q_{n-2}, \qquad (4.1)$$

and take $R = p_n^2 - D\,q_n^2$ until R becomes either of ± 1. It is known that at $(n=k-1)$th step R becomes $+1$ and -1, respectively, for even and odd k. The results are given in Table 1 for D=61. Though several numerals are omitted, they can be reproduced by following (4.1).

Selenius rediscovered the essence of the algorithm by Bhaskara II who completed the old Hindu method for solving this problem, and declared that by using Chakrava (cyclic) method it takes much fewer steps before reaching the final result.[11] The underlined columns of n in Table 1 are the ones which are taken by Chakrava method. Namely only about two thirds of the whole steps of the iterative algorithm are necessary. However, this method becomes powerful for D whose continued fractions expansion contains long consecutive 1's as

$$\sqrt{115} = [10, \overline{1,2,1,1,1,1,1,2,1,20}].$$

Notwithstanding of these arguments the present method is far more superior than any other proposed method

Table 1. Conventional procedure for solving the Pellep-1 for D=61. Smallest solutions of Llep-1 and Pell-1 appear in row 10 and 21, respectively. Omitted numerals in rows 15-21 can be obtained by using the numerals given here.

n	a_n	p_n	q_n	$R=p_n^2-D\,q_n^2$
0	7	7	1	$7^2-61\times1^2=-12$
1	1	$7\times1+1=8$	$1\times1=1$	$8^2-61\times1^2=3$
2	4	$8\times4+7=39$	$1\times4+1=5$	$39^2-61\times5^2=-4$
3	3	$39\times3+8=125$	$5\times3+1=16$	$125^2-61\times16^2=9$
4	1	$125\times1+39=164$	$16\times1+5=21$	$164^2-61\times21^2=-5$
5	2	$164\times2+125=453$	$21\times2+16=58$	$453^2-61\times58^2=5$
6	2	$453\times2+164=1070$	$58\times2+21=137$	$1070^2-61\times137^2=-9$
7	1	$1070\times1+453=1523$	$137\times1+58=195$	$1523^2-61\times195^2=4$
8	3	$1523\times3+1070=5639$	$195\times3+137=722$	$5639^2-61\times722^2=-3$
9	4	$5639\times4+1523=24079$	$722\times4+195=3083$	$24079^2-61\times3083^2=12$
10	1	$24079\times1+5639=29718$	$3083\times1+722=3805$	$29718^2-61\times3805^2=-1$
11	14	$29718\times14+24079=440131$	$3805\times14+3083=56353$	$440131^2-61\times56353^2=12$
12	1	$440131\times1+29718=469849$	$56353\times1+3805=60158$	$469849^2-61\times60158^2=-3$
13	4	$469849\times4+440131=2319527$	$60158\times4+56353=296985$	$2319527^2-61\times296985^2=4$
14	3	$2319527\times3+469849=7428430$	$296985\times3+60158=951113$	$7428430^2-61\times951113^2=-9$
15	1	9747957	1248098	5
16	2	26924344	3447309	−5
17	2	63596645	8142716	9
18	1	90520989	11590025	−4
19	3	335159612	42912791	3
20	4	1431159437	183241189	−12
21	1	1766319049	226153980	1
22	14	26159626123	3349396909	−12

The advantage of the present algorithm over other conventional methods lies in the transformation of the continuant into the caterpillar graph and its Z-counting. For demonstrating this fact see Fig. 4, where the lower members of p_n and q_n's are compared with the corresponding caterpillars and their Z values. Important role of the topological index Z has been found in a number of problems not only in elementary mathematics but also in

algebraic number theory, such as in the problems of Pythagorean and Heronian triangles, Pascal's triangle, rational number approximation of quadratic irrational numbers, etc.[18,19)]

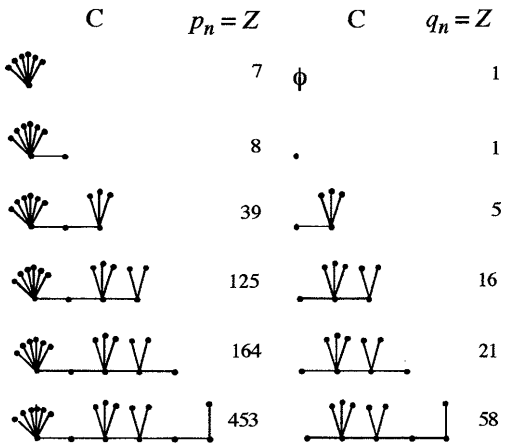


Fig. 4. Caterpillars and their Z-values conveging to the solution of Pellep-1 with D=61. Compare with Table 1.

References

1) H. Hosoya and N. Asamoto, *Natural Sci. Rept. Ochanomizu Univ.*, **57** (2006) (1) 57.

2) H. Hosoya, *Natural Sci. Rept. Ochanomizu Univ.*, **57** (2006) (2) 19.

3) H. Hosoya, *Natural Sci. Rept. Ochanomizu Univ.*, **57** (2006) (2) 35.

4) H. Hosoya, *Natural Sci. Rept. Ochanomizu Univ.*, **58** (2007) in print.

5) A. H. Beiler, Recreations in the Theory of Numbers. The Queen of Mathematics Entertains. Dover, New York (1964), pp. 248.

6) E. J. Barbeau, Pell's Equation. Springer, New York (2002), pp.55.

7) T. Takagi, Elementary Number Theory (in Japanese), Kyoritsu, Tokyo (1931), pp. 124.

8) D. E. Knuth, The Art of Computer Programming, Vol. 1, Addison-Wesley, Reading, MS (1968), pp. 339.

9) R. L. Graham, D. E. Knuth, and O. Patashnik, Concrete Mathematics. A Foundation for Computer Science, Addison-Wesley, Reading, MS (1989), pp. 287.

10) A. T. Benjamin and J. J. Quinn, Proofs That Really Count. The Art of Combinatorial Proof, Mathematical Association of America, Washington, D. C., 2003, p. 57.

11) C.-O. Selenius, Historia Math., **2** (1975) 167.

12) H. Hosoya, *Bull. Chem. Soc. Jpn.*, **44** (1971) 2332.

13) H. Hosoya, *Fibonacci Quart.*, **11** (1973) 255.

14) K. H. Rosen, J. G. Michaels, J. L. Gross, J. W. Grossman, and D. R. Shier (Eds.), Handbook of Discrete and Combinatorial Mathematics, CRC Press, Boca Raton, FL (2000), p. 498.

15) E. W. Weisstein, CRC Concise Encyclopedia of Mathematics, Chapman & Hall/CRC, Boca Raton, FL (2003), p. 351.

16) V. E. Hoggatt, Jr., Fibonacci and Lucas Numbers, Houghton Mifflin, Boston (1969).

17) T. Koshy, Fibonacci and Lucas Numbers with Applications, Wiley, New York (2001).

18) H. Hosoya, *Croat. Chem. Acta*, **80** (2007) 239.

19) H. Hosoya, *J. Chem. Inf. Mod.*, **47** (2007) 744.