JOURNAL OF THE TENNESSEE ACADEMY OF SCIENCE 67(4):65-69 OCTOBER 1992

# FIBONACCI-TYPE RELATIONS AMONG SOLUTIONS TO THE PELL EQUATION

L. M. HIVELY, V. R. R. UPPULURI, AND W. G. MCMILLAN

*Applied Technology Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-7294*
*130 Indian Lane, Oak Ridge, TN 37830*
*Department of Chemistry and Biochemistry, University of California, Los Angeles, CA 90024*

**ABSTRACT--Three Fibonacci forms are obtained as recursion relations among the integer solutions to the Pell equation, $x^2 - Dy^2 = 1$, which has $x_1 = p$ and $y_1 = q$ as the first nontrivial solution. The first form is $x_{n+1} = px_n + Dqy_n$ and $y_{n+1} = qx_n + py_n$. The second form is $z_{n+2} = 2pz_{n+1} - z_n$, where z can be x or y. The third form involves products: $x_nx_{n+1} = Dy_ny_{n+1} + p$. Asymptotic forms are obtained in the limit of large n: $x_{n+1}/x_n = y_{n+1}/y_n = p + qD^{1/2}$, and $x_n/y_n = D^{1/2}$. Relationships between the solutions are found for $D = EF^2$ and $D = E$. Recursion sequences are found for $\mathrm{mod}_m(x_n)$ and for $\mathrm{mod}_m(y_n/q)$ and depend only on $\mathrm{mod}_m p$. The cases of D = 3, 12, and 27 are presented in more detail as examples.**

A question in the ORNL Review (Uppuluri, 1988) motivated this work: "For any set of seven consecutive integers, the mean and the standard deviation are also integers; find other sets of integers sharing this property (Delany, 1989)." Since any set of x consecutive integers, for x even, will have a half-integer mean, only an odd number (x = 2j + 1) of consecutive integers satisfies the integer mean requirement. The standard deviation, y, of this sequence (N -j, N - j +1, .., N - 1, N, N + 1, .., N + j) is found from:

$$y^2 = 2(1^2 + 2^2 + \dots + j^2)/(2j + 1) = j(j + 1)/3. \quad (1)$$

Solving equation (1) for x = 2j + 1 yields the "Pell equation" for D = 12: $x^2 - Dy^2 = 1$; Table 1 shows the first 16 nontrivial (integer) solutions to this equation. We further note that the starred values of x in Table 1 denote solutions, which, when multiplied by two, constitute the series used by Lehmer (1935), $u_n = u^2_{n-1} - 2$, as a test for primality of Mersenne's numbers.

Most books in number theory discuss the Pell equation and its solutions. The general topic of linear recursions (discussed later) is also well known; see Lidle and Nieferreiter (1986:chapter 6) for example. Here, we discuss special case solutions, for which only general forms are published. The Pell equation has the form $x^2 - Dy^2 = 1$, where x, y, and D are integers; the integer solutions are (Beiler, 1964):

$$x_n = [(p + qD^{1/2})^n + (p - qD^{1/2})^n]/2 \quad (2a)$$

$$y_n = [(p + qD^{1/2})^n - (p - qD^{1/2})^n]/2D^{1/2}. \quad (2b)$$

For all values of D, x = 1 and y = 0 are trivial solutions; the first nontrivial solution is $x_1 = p$ and $y_1 = q$. When D is the square of an integer (D = $w^2$), the Pell equation takes the form $x^2 - w^2y^2 = x^2 - u^2 = 1$ for x and u both integers. It is well known that no nontrivial solutions exist in this case, because two successive integers, m and m + 1, yield the smallest difference (2m + 1 = 1) between integers squared, when m = 0. Therefore, these values of D are omitted from further discussion.

Equations (2a) and (2b) are easily solved (Chrystal, 1964:480, equation 6) for $(p + qD^{1/2})^n$ and $(p - qD^{1/2})^n$ as follows:

$$(p + qD^{1/2})^n = x_n + D^{1/2}y_n \quad (3a)$$

$$(p - qD^{1/2})^n = x_n - D^{1/2}y_n. \quad (3b)$$

The first Fibonacci form is obtained by substituting equations (3a) and (3b) into equations (2a) and (2b) for the (n + 1)st solution:

$$x_{n+1} = [(p + qD^{1/2})(x_n + D^{1/2}y_n) + (p - qD^{1/2})(x_n - D^{1/2}y_n)]/2 = px_n + qDy_n \quad (4a)$$

$$y_{n+1} = [(p + qD^{1/2})(x_n + D^{1/2}y_n) - (p - qD^{1/2})(x_n - D^{1/2}y_n)]/2D^{1/2} = qx_n + py_n. \quad (4b)$$

The advantage of these recursions is that they can be easily programmed on a computer or calculator to determine the solutions to the Pell equation (see Tables 1-3, for example). Adler (1972) obtained equivalent forms for D = 3. A second Fibonacci form is obtained by using the (n+2) and (n+1) forms of equations (3a) and (3b) to eliminate the cross terms, where z = x or y:

$$z_{n+2} = 2pz_{n+1} + (Dq^2 - p^2)z_n = 2pz_{n+1} - z_n. \quad (5)$$

A third Fibonacci relation is obtained by multiplying equation (4a) by $x_n$ and subtracting equation (4b) times $Dy_n$. Using the Pell equation to eliminate two terms, a product form is:

$$x_nx_{n+1} = Dy_ny_{n+1} + p. \quad (6)$$

Several asymptotic forms can be obtained from equations (4a) and (4b). By dividing the Pell equation by $y_n$, in the limit of very large values of n, the form is obviously:

$$\lim_{n\to\infty} x_n/y_n = D^{1/2}. \quad (7)$$

Dividing equation (4a) by $x_n$ and substituting from (7), a second form is obtained:

$$\lim_{n\to\infty} x_{n+1}/x_n = p + qD^{1/2}.$$

By dividing equation (4b) by $y_n$ and substituting from (7), a third limit is:

$$\lim_{n\to\infty} y_{n+1}/y_n = p + qD^{1/2}. \quad (9)$$

The last two asymptotic forms, in the limit of large values of n, can be written in three different forms:

$$\lim_{n\to\infty} x_{n+1}/x_n = \lim_{n\to\infty} y_{n+1}/y_n = p + qD^{1/2} \quad (10a)$$

$$= p + (p^2 - 1)^{1/2} \quad (10b)$$

$$= (1 + Dq^2)^{1/2} + qD^{1/2}. \quad (10c)$$

The forms in equations (10b) and (10c) are obtained by substitution from the first nontrivial solution of the Pell equation. Alternatively, we note that $(p + qD^{1/2})(p - qD^{1/2}) = 1$ and $|p - qD^{1/2}| < 1$, imply that the dominant term for large n in equations (2a) - (2b) is $|p + qD^{1/2}| > 1$, thus giving equation (10a) directly. These asymptotic limits are satisfied to ≥7 decimal places for n > 3.

TABLE 1. First 16 nontrivial solutions to Pell equation (D = 12).

| n | $x_n$ | $y_n$ |
|---|---|---|
| 1 | 7* | 2 |
| 2 | 97* | 28 |
| 3 | 1 351 | 390 |
| 4 | 18 817 | 5 432 |
| 5 | 262 087 | 75 658 |
| 6 | 3 650 401 | 1 053 780 |
| 7 | 50 843 527 | 14 677 262 |
| 8 | 708 158 977* | 204 427 888 |
| 9 | 9 863 382 151 | 2 847 313 170 |
| 10 | 137 379 191 137 | 39 657 956 492 |
| 11 | 1 913 445 293 767 | 552 364 077 718 |
| 12 | 26 650 854 921 601 | 7 693 439 131 560 |
| 13 | 371 198 523 608 647 | 107 155 783 764 122 |
| 14 | 5 170 128 475 599 457 | 1 492 487 533 566 148 |
| 15 | 72 010 600 134 783 751 | 20 787 669 686 161 950 |
| 16 | 1 002 978 273 411 373 057* | 289 534 888 072 701 152 |

*Denote solutions, which, when multiplied by two, constitute the series used by Lehmer (1935), $u_n = u^2_{n-1} - 2$, as a test for primality of Mersenne's numbers.

TABLE 2. First 33 non-trivial solutions to Pell equation (D = 3).

| n | $x_n$ | $y_n$ |
|---|---|---|
| 1 | 2 | 1 |
| 2 | 7 | 4 |
| 3 | 26 | 15 |
| 4 | 97 | 56 |
| 5 | 362 | 209 |
| 6 | 1 351 | 780 |
| 7 | 5 042 | 2 911 |
| 8 | 18 817 | 10 864 |
| 9 | 70 226 | 40 545 |
| 10 | 262 087 | 151 316 |
| 11 | 978 122 | 564 719 |
| 12 | 3 650 401 | 2 107 560 |
| 13 | 13 623 482 | 7 865 521 |
| 14 | 50 843 527 | 29 354 524 |
| 15 | 189 750 626 | 109 552 575 |
| 16 | 708 158 977 | 408 855 776 |
| 17 | 2 642 885 282 | 1 525 870 529 |
| 18 | 9 863 382 151 | 5 694 626 340 |
| 19 | 36 810 643 322 | 21 252 634 831 |
| 20 | 137 379 191 137 | 79 315 912 984 |
| 21 | 512 706 121 226 | 296 011 017 105 |
| 22 | 1 913 445 293 767 | 1 104 728 155 436 |
| 23 | 7 141 075 053 842 | 4 122 901 604 639 |
| 24 | 26 650 854 921 601 | 15 386 878 263 120 |
| 25 | 99 462 344 632 562 | 57 424 611 447 841 |
| 26 | 371 198 523 608 647 | 214 311 567 528 244 |
| 27 | 1 385 331 749 802 026 | 799 821 658 665 135 |
| 28 | 5 170 128 475 599 457 | 2 984 975 067 132 296 |
| 29 | 19 295 182 152 595 802 | 11 140 078 609 864 049 |
| 30 | 72 010 600 134 783 751 | 41 575 339 372 323 900 |
| 31 | 268 747 218 386 539 202 | 155 161 278 879 431 551 |
| 32 | 1 002 978 273 411 373 057 | 579 069 776 145 402 304 |
| 33 | 3 743 165 875 258 953 026 | 2 161 117 825 702 177 665 |

TABLE 3. First 11 nontrivial solutions to Pell equation (D = 27).

| n | $x_n$ | $y_n$ |
|---|---|---|
| 1 | 26 | 5 |
| 2 | 1 351 | 260 |
| 3 | 70 226 | 13 515 |
| 4 | 3 650 401 | 702 520 |
| 5 | 189 750 626 | 36 517 525 |
| 6 | 9 863 382 151 | 1 898 208 780 |
| 7 | 512 706 121 226 | 98 670 339 035 |
| 8 | 26 650 854 921 601 | 5 128 959 421 040 |
| 9 | 1 385 331 749 802 026 | 266 607 219 555 045 |
| 10 | 72 010 600 134 783 751 | 13 858 446 457 441 300 |
| 11 | 3 743 165 875 258 953 026 | 720 372 608 567 392 555 |

Study of Tables 1 to 3 reveals that the n-th Pell solution, $(x_n, y_n)$ for a given value of $D = EF^2$, is related to the solution for D = E since the Pell equation can be rewritten as:

$$x^2 - Dy^2 = x^2 - E(Fy)^2 = 1. \quad (11)$$

The general relationship between solutions can be written as:

$$x_{mn}(D = E)/x_n(D = EF^2) = 1 \quad (12a)$$

$$y_{mn}(D = E)/y_n(D = EF^2) = F, \quad (12b)$$

where m is the appropriate multiple, based on where the first nontrivial solution for $D = EF^2$ occurs relative to D = E. For example, for $D = 27 = 3(3)^2$, the relationships are (see Table 3):

$$x_{3n}(D = 3)/x_n(D = 27) = 1 \quad (13a)$$

$$y_{3n}(D = 3)/y_n(D = 27) = 3. \quad (13b)$$

The value of m = 3 occurs because the first nontrivial solution for D = 27 is (p = 26, q = 5), corresponds to the third solution ($x_3 = 26$, $y_3 = 15$) for D = 3 (Table 2). Recursion sequences are discussed next.

Table 4 lists the first nontrivial solutions to the Pell equation for $D \leq 27$. The higher order Pell solutions, $(x_n, y_n)$ have a resursion in the right-most digit (RMD) of both $x_n$ and $y_n$ for a fixed value of D. Examples of these recursions are shown in the two right columns of Table 4 and are readily seen in Tables 1 to 3 for D-values of 3, 12, 27, respectively.

We note that the recursion for RMD($x_n$) is a function of the RMD of $x_1 = p$, RMD(p), as shown in Table 5. The recursion for $x_n$ always begins with (1, RMD(p),..), because $(x_0 y_0) = (1,0)$ is the (n = 0) trivial solution and $(x_1, y_1) = (p, q)$ is the first (n = 1) nontrivial solution, and ends in RMD(p). The sequence length is 1 to 6 digits, but no lengths of 5 occur. The digits (0 2 3 5 7 8) occur only in pairs, while the digits (1 4 6 9) occur only alone. No all even sequences occur. Even-odd recursions alternate even and odd and begin with an even digit.

Proof that the RMD recursion is a function of the RMD(p) only relies on showing a stronger property. Namely, the $x_n$ sequence is a function of p only, which can be easily shown as follows. Substitute $x_1 = p$ and $y_1 = q$ into (4a) to obtain:

$$x_2 = 2p^2 - 1. \quad (14)$$

Now, substitute $x_1 = p$ and $x_2$ from (14) into (5) to obtain:

$$x_3 = 4p^3 - 3p. \quad (15)$$

Successive substitutions of $x_n$ and $x_{n+1}$ into (5) yield:

$$x_4 = 8p^4 - 8p^2 + 1 \quad (16)$$

$$x_5 = 16p^5 - 20p^3 + 5p \quad (17)$$

$$x_6 = 32p^6 - 48p^4 + 18p^2 - 1. \quad (18)$$

The general form for $x_n$ can be obtained by expressing (2a) as:

$$x_n = \sum_{k\ \mathrm{even}}^{n} \binom{n}{k} (qD^{1/2})^k p^{n-k}. \quad (19)$$

Substituting $Dq^2 = p^2 - 1$ from the Pell equation into (19) yields a form

TABLE 4. First nontrivial solutions to the Pell equation for D < 27 and right-most digit recursions beginning with the first (n = 1) nontrivial solution.

| D | x = p | y = q | $x_n$ recursion | $y_n$ recursion |
|---|---|---|---|---|
| 2 | 3 | 2 | 3 7 9 7 3 1 | 2 2 0 8 8 0 |
| 3 | 2 | 1 | 2 7 6 7 2 1 | 1 4 5 6 9 0 |
| 5 | 9 | 4 | 9 1 | 4 2 2 4 0 6 8 8 6 0 |
| 6 | 5 | 2 | 5 9 5 1 | 2 0 8 0 |
| 7 | 8 | 3 | 8 7 4 7 8 1 | 3 8 5 2 7 0 |
| 8 | 3 | 1 | 3 7 9 7 3 1 | 1 6 5 4 9 0 |
| 10 | 19 | 6 | 9 1 | 6 8 8 6 0 4 2 2 4 0 |
| 11 | 10 | 3 | 0 9 0 1 | 3 0 7 0 |
| 12 | 7 | 2 | 7 7 1 | 2 8 0 |
| 13 | 649 | 180 | 9 1 | 0 |
| 14 | 15 | 4 | 5 9 5 1 | 4 0 6 0 |
| 15 | 4 | 1 | 4 1 | 1 8 3 6 5 4 7 2 9 0 |
| 17 | 33 | 8 | 3 7 9 7 3 1 | 8 8 0 2 2 0 |
| 18 | 17 | 4 | 7 7 1 | 4 6 0 |
| 19 | 170 | 39 | 0 9 0 1 | 9 0 1 0 |
| 20 | 9 | 2 | 9 1 | 2 6 6 2 0 8 4 4 8 0 |
| 21 | 55 | 12 | 5 9 5 1 | 2 0 8 0 |
| 22 | 197 | 42 | 7 7 1 | 2 8 0 |
| 23 | 24 | 5 | 4 1 | 5 0 |
| 24 | 5 | 1 | 5 9 5 1 | 1 0 9 0 |
| 26 | 51 | 10 | 1 | 0 |
| 27 | 26 | 5 | 6 1 | 5 0 |

that is a function of p only:

$$x_n = \sum_{k\ \mathrm{even}}^{n} \sum_{j=0}^{k/2} \binom{n}{k} \binom{k/2}{j} (-1)^j p^{n-2j}. \quad (20)$$

Since the $x_n$ sequence is a function of p only and depends only on additions, subtractions, and multiplications, successive operations produce the recursions. Thus, the final step of the proof requires listing all the possibilities for RMD(p) as shown in Table 5.

Table 4 shows the recursion for $y_n$ as a function of p and q in general. However, simplified recursions for $y_n/q$ can be found by substituting $x_1 = p$ and $y_1 = q$ into (4b) to obtain:

$$y_2 = 2pq. \quad (21)$$

As before, successive substitutions of $y_n$ and $y_{n+1}$ into (5) yield:

TABLE 5. RMD recursion for $x_n$ and $y_n/q$ versus RMD of p, beginning with the trivial (n = 0) solution.

| RMD (p) | Recursion for RMD($x_n$) | Recursion for RMD($y_n/q$) |
|---|---|---|
| 0 | 1 0 9 0 | 0 1 0 9 |
| 1 | 1 | 0 1 2 3 4 5 6 7 8 9 |
| 2 | 1 2 7 6 7 2 | 0 1 4 5 6 9 |
| 3 | 1 3 7 9 7 3 | 0 1 6 5 4 9 |
| 4 | 1 4 | 0 1 8 3 6 5 4 7 2 9 |
| 5 | 1 5 9 5 | 0 1 0 9 |
| 6 | 1 6 | 0 1 2 3 4 5 6 7 8 9 |
| 7 | 1 7 7 | 0 1 4 5 6 9 |
| 8 | 1 8 7 4 7 8 | 0 1 6 5 4 9 |
| 9 | 1 9 | 0 1 8 3 6 5 4 7 2 9 |

$$y_3 = q(4p^2 - 1) \quad (22)$$
$$y_4 = q(8p^3 - 4p) \quad (23)$$
$$y_5 = q(16p^4 - 12p^2 + 1) \quad (24)$$
$$y_6 = q(32p^5 - 32p^3 + 6p). \quad (25)$$

The general form for $y_n$ can be obtained by expressing (2b) as:

$$y_n = D^{-1/2} \sum_{k\ \mathrm{odd}}^{n} \binom{n}{k} (qD^{1/2})^k p^{n-k}. \quad (26)$$

As before, substitution of $Dq^2 = p^2 - 1$ into (24) yields:

$$y_n/q = \sum_{k\ \mathrm{odd}}^{n} \sum_{j=0}^{(k-1)/2} \binom{n}{k} \binom{(k-1)/2}{j} (-1)^j p^{n-2j-1}. \quad (27)$$

Since the $y_n/q$ sequence is a function of p only and depends only on additions, subtractions, and multiplications, successive operations produce the recursions. Thus, the final step of this proof requires listing all the possibilities for RMD(p) as shown in Table 5. As before, $(x_0, y_0) = (1, 0)$ is the (n = 0) trivial solution, $(x_1, y_1/q) = (p, 1)$ and $(x_2, y_2/q) = (x_2, 2p)$ are the first (n = 1) and second (n = 2) nontrivial solutions, so the recursion always begins with (0, 1, RMD(2p)..). The recursion for $y_n/q$ always ends in 9. The sequence length is 4, 6, or 10 digits. The digit (0) occurs both alone and in pairs; other digits occur only alone. All sequences occur as even-odd recursions alternating even and odd.

The $y_n$-recursions for RMD(p) = 1 and 6 are identical, as are those for (2 and 7), (3 and 8), (4 and 9), and (5 and 0). The paired nature of these five different recursion sequences arises because the RMD(p) is simply $\mathrm{mod}_m p$, with m = 10 = 5 x 2. Table 6 shows the recursions for $\mathrm{mod}_m(x_n)$ and $\mathrm{mod}_m(y_n/q)$ versus $\mathrm{mod}_m p$ for $2 \leq m \leq 13$ and m = prime; for ease of notation, we use A = 10, B = 11, C = 12. The modulo-m recursions can be generalized somewhat as shown in Table 7. Some other generalities can also be made. The recursions for $\mathrm{mod}_m(x_n)$ and $\mathrm{mod}_m(y_n/q)$ begin with (1, $\mathrm{mod}_m p$,...) and (0, 1, and $\mathrm{mod}_m 2p$,...), respectively, as determined from equations (20) and (27). The recursions for $\mathrm{mod}_m(x_n)$ and $\mathrm{mod}_m(y_n/q)$ end with $\mathrm{mod}_m p$ and (m - 1), respectively.

TABLE 6. Recursions for $\mathrm{mod}_m(x_n)$ and $\mathrm{mod}_m(y_n/q)$ versus $\mathrm{mod}_m p$ for 2 < m < 13 and m = prime beginning with the trivial (n = 0) solution to the Pell equation. The letters (A, B, C) designate (10, 11, 12), respectively.

| m | $\mathrm{mod}_m p$ | $\mathrm{mod}_m(x_n)$ | $\mathrm{mod}_m(y_n/q)$ |
|---|---|---|---|
| 2 | 0 | 10 | 01 |
| | 1 | 1 | 01 |
| 3 | 0 | 1020 | 0102 |
| | 1 | 1 | 012 |
| | 2 | 12 | 011022 |
| 5 | 0 | 1040 | 0104 |
| | 1 | 1 | 01234 |
| | 2 | 122 | 014 |
| | 3 | 132423 | 011044 |
| | 4 | 14 | 0133104224 |
| 7 | 0 | 1060 | 0106 |
| | 1 | 1 | 0123456 |
| | 2 | 12056502 | 01410636 |
| | 3 | 133 | 016 |
| | 4 | 143634 | 011066 |
| | 5 | 15026205 | 01310646 |
| | 6 | 16 | 0153351062... |
| 11 | 0 | 10A0 | 010A |
| | 1 | 1 | 0123456789A |
| | 2 | 12749A9472 | 014410A77A |
| | 3 | 136058A85063 | 0162610A595A |
| | 4 | 14927A7294 | 018810A33A |
| | 5 | 155 | 01A |
| | 6 | 165A56 | 0110AA |
| | 7 | 17997 | 0138A |
| | 8 | 180653A35068 | 0152510A696A |
| | 9 | 19779 | 0174A |
| | A | 1A | 019375573910A28... |
| 13 | 0 | 10C0 | 010C |
| | 1 | 1 | 0123456789ABC |
| | 2 | 12706BCB6072 | 0142410C9B9C |
| | 3 | 134859ACA95843 | 01699610C7447C |
| | 4 | 145AA54 | 018B25C |
| | 5 | 15A44A5 | 01A853C |
| | 6 | 166 | 01C |
| | 7 | 176C67 | 0110CC |
| | 8 | 18A9435C5349A8 | 01388310CA55AC |
| | 9 | 1953A84C48A359 | 015B510C8228C |
| | A | 1A4554A | 017946C |
| | B | 1B7062C2607B | 0192910C4B4C |
| | C | 1C | 01B3957... |

## ACKNOWLEDGMENTS

This manuscript has been authored by a contractor of the United States Government under contract DE-AC05-84OR21400. Accordingly, the United States Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for United States Government purposes. The manuscript was prepared by the Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-7294, operated by Martin Marietta Energy Systems, Inc., for the United States Department of Energy under contract DE-AC05-84OR21400. V. R. R. Uppuluri is retired from the Engineering Physics and Mathematics Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee.

TABLE 7. Generalized modulo-m recursions.

| $mod_m p$ | $mod_m(x_n)$ | $mod_m(y_n/q)$ |
|---|---|---|
| 0 | 1 0 z 0 | 0 1 0 z |
| 1 | 1 | 0 1 2 3...z |
| r = (m - 1)/2 | 1 r r | 0 1 z |
| s = (m + 1)/2 | 1 s r z r s | 0 1 1 0 z z |
| z = (m - 1) | 1 z | |

## LITERATURE CITED

ADLER, I. 1972. Three diophantine equations--part II. Fibonacci Quarterly, 7:181-193.

BEILER, A. H. 1964. Recreations in the theory of numbers. Dover Publications, Inc., New York.

CHRYSTAL, G. 1964. Algebra: an elementary textbook for the higher classes of secondary schools and for colleges. Seventh ed. Chelsea Publishers, New York, vol. 2.

DELANY, J. 1989. Problems and solutions. Amer. Math. Monthly, 96:54.

LIDL, R., AND H. NIEDERREITER. 1986. Introduction to finite fields and their applications. Cambridge Univ. Press, Cambridge, Massachusetts.

LEHMER, D. H. 1935. On Lucas's test for the primality of Mersenne's numbers. J. London Math. Soc., 10:162-171.

UPPULURI, V. R. R. 1988. Take a number. ORNL Review, 21:97.