ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY

Please send all communucations concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN UNIVERSITY, LOCK HAVEN, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, all solutions should be submitted on separate signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-385 *Proposed by M. Wachtel, Zurich, Switzerland*

Solve the following system of equations:

I. $U_{f(n)}^2 + V_{g(n)}^2 - 3 \cdot U_{f(n)}V_{g(n)} = 1;$

II. $3 \cdot U_{h(n)}V_{i(n)} - (U_{h(n)}^2 + V_{i(n)}^2) = 1.$

H-386 *Proposed by Paul S. Bruckman, Fair Oaks, CA*

Define the multiple-valued *Fibonacci function* ${}^mF : \mathbf{C} \to \mathbf{C}$ as follows:

1. ${}^mF(z) = \frac{1}{\sqrt{5}}(\exp Lz - \exp L'z)$, $z \in \mathbf{C}$, $m \in \mathbb{Z}$,

where $L = \log \alpha$, $\alpha = \frac{1}{2}(1 + \sqrt{5})$, $L' = (2m + 1)i\pi - L$, and "log" denotes the principal logarithm.

a. Show that ${}^mF(n) = F_n$ for all integers m and n.

b. Prove the multiplication formula

2. $\prod_{m=0}^{n-1} {}^mF\left(k + \frac{r}{n}\right) = 5^{-\frac{1}{2}(n-1)}F_{nk+r}$, where n, k, r are integers with $0 < r < n$.

c. With m fixed, find the zeros of ${}^mF$.

H-387 *Proposed by Lawrence Somer, Washington, D.C.*

Let $\{w_n\}_{n=0}^{\infty}$ be a second-order linear integral recurrence defined by the recursion relation

$$w_{n+2} = aw_{n+1} + bw_n,$$

where $b \neq 0$. Show the following:

(i) If p is an odd prime such that $p \nmid b$ and $w_1^2 - w_0w_2$ is a quadratic nonresidue of p, then

$$p \nmid w_{2n} \quad \text{for any } n \geqslant 0.$$

(ii) If p is an odd prime such that $(-b)(w_1^2 - w_0 w_2)$ is a quadratic nonresidue of p, then

$$p \nmid w_{2n+1} \quad \text{for any } n \geqslant 0.$$

(iii) If p is an odd prime such that $-b$ is a nonzero quadratic residue of and $w_1^2 - w_0 w_2$ is a quadratic nonresidue of p, then

$$p \nmid w_n \quad \text{for any } n \geqslant 0.$$

H-388 *Proposed by Piero Filipponi, Rome, Italy*

This problem arose in the determination of the diameter of a class of locally restricted digraphs [1].

For a given integer $n \geqslant 2$, let $P_1 = \{p_{1,1}, p_{1,2}, \ldots, p_{1,k_1}\}$ be a nonempty (i.e., $k_1 \geqslant 1$) increasing sequence of positive integers such that $p_{1,k_1} \leqslant n - 1$. Let $P_2 = \{p_{2,1}, p_{2,2}, \ldots, p_{2,k_2}\}$ be the increasing sequence containing all nonzero distinct values given by $p_{1,i} + p_{1,j} \pmod n$ $(i, j = 1, 2, \ldots, k_1)$. In general let $P_h = \{p_{h,1}, p_{h,2}, \ldots, p_{h,k_h}\}$ be the increasing sequence containing all nonzero distinct values given by $p_{h-1,i} + p_{1,j} \pmod n$ $(i = 1, 2, \ldots, k_{n-1}$, $j = 1, 2, \ldots, k_1)$. Furthermore, let B_m $(m = 1, 2, \ldots)$ be the increasing sequence containing all values given by

$$\bigcup_{j=1}^{m} P_j.$$

Find, in terms of n, $p_{1,1}, \ldots, p_{1,k_1}$, the smallest integer t such that

$$B_t = \{1, 2, \ldots, n - 1\}.$$

Remark: The necessary and sufficient condition for t to exist (i.e., to be finite) is given in [1]:

$$\gcd(n, p_{1,1}, \ldots, p_{1,k_1}) = 1.$$

In such a case we have $1 \leqslant t \leqslant n - 1$. It is easily seen that

$$k_1 = 1 \Longleftrightarrow t = n - 1$$

$$k_1 = n - 1 \Longleftrightarrow t = 1;$$

furthermore, it can be conjectured that either $t = n - 1$ or $1 \leqslant t \leqslant [n/2]$.

Reference

1. P. Filipponi. "Digraphs and Circulant Matrices." *Ricerca Operativa*, no. 17 (1981):41-62.

An Example

$n = 8$ $P_1 = \{3, 5\}$ $\rightarrow B_1 = \{3, 5\}$

$P_2 = \{2, 6\}$ $\rightarrow B_2 = \{2, 3, 5, 6\}$

$P_3 = \{1, 3, 5, 7\}$ $\rightarrow B_3 = \{1, 2, 3, 5, 6, 7\}$

$P_4 = \{2, 4, 6\}$ $\rightarrow B_4 = \{1, 2, 3, 4, 5, 6, 7\}$; hence, we have $t = 4$.

SOLUTIONS

A Note to Solutions of H-350, H-354 by Paul Bruckman

H-350

Although the published solution is apparently correct, it can be considerably simplified. In the course of solving H-372, it occurred to the solver that the same method of solution could have been applied to solve H-350 (but was not). As noted in the published solution, the given equation:

$$5y^2 - Ax^2 = 1 \quad (\text{where } A \equiv 5a^2 + 5a + 1) \tag{1}$$

has general solutions

$$x_n = \frac{u^{2n-1} - v^{2n-1}}{2\sqrt{A}}, \quad y_n = \frac{u^{2n-1} + v^{2n-1}}{2\sqrt{5}}, \quad n = 1, 2, \ldots,$$
$$\text{where } u \equiv (2a + 1)\sqrt{5} + 2\sqrt{A}, \quad v \equiv (2a + 1)\sqrt{5} - 2\sqrt{A}. \tag{2}$$

Note $uv = 1$. From (2), we could easily have derived the following relations:

$$5y_n y_{n+1} - Ax_n x_{n+1} = B \equiv 40a^2 + 40a + 9; \tag{3}$$

$$x_{n+1}y_n - x_n y_{n+1} = 4(2a + 1). \tag{4}$$

Dividing (3) and (4) throughout by $y_n y_{n+1}$ would have yielded the following:

$$5 - Ar_n r_{n+1} = B/y_n y_{n+1}, \quad r_{n+1} - r_n = 4(2a + 1)/y_n y_{n+1},$$

or

$$5 - Ar_n r_{n+1} = \frac{B}{4(2a + 1)}(r_{n+1} - r_n),$$

which yields:

$$r_{n+1} = \frac{Br_n + 20(2a + 1)}{4A(2a + 1)r_n + B}, \quad \text{with } r_1 = 2/(2a + 1). \tag{5}$$

The expression given by (5) is a recursion of the first order (though modular rather than linear), which is considerably simpler than the cumbersome third-order recursion published as the solution. The published third-order recursion follows from (5) (after some computation), but not vice-versa.

H-354

The published "solution" is not a solution (or even an attempted solution) of the original problem, as submitted. The original problem asked for necessary and sufficient conditions for a solution in integers (x, y) to exist for the equation:

$$ax^2 - by^2 = c, \tag{1}$$

where a, b, c are pairwise relatively prime positive integers such that ab is not a perfect square. It is already known that if a solution of (1) exists, then infinitely many such solutions exist. Moreover, an explicit formula for all such solutions is known, in terms of the one known solution (if any).

In the published "solution" to the problem, as *altered*, Wächtel changed the notation to the following equation,

$$By^2 - Ax^2 = C, \tag{2}$$

which in itself is not a substantive modification; however, he also indicated

that C is to be *dependent* on A and B. Nothing of the sort was intended by the proposer; in the original problem, a, b, and c are *independently arbitrary*, subject only to the conditions noted above. Moreover, Wächtel attempted *construction* of the solutions to particular cases. This again was not the intent of the proposer, although admittedly the construction of the *minimal* solution, if possible, would go a long way toward solving the problem.

The only progress made by the proposer toward solution of the original problem may be summarized as follows:

I. *Necessary* conditions for a solution of (1) to exist are the following, in terms of the generalized Legendre symbols:

$$\left(\frac{ac}{b}\right) = \left(\frac{-bc}{a}\right) = \left(\frac{ab}{c}\right) = 1. \tag{3}$$

That the conditions in (3) are not sufficient may be demonstrated from the counter-example: $a = 1$, $b = 17$, $c = 2$, in this case, $x^2 - 17y^2 = 2$ has no solution, yet the conditions in (3) are satisfied.

II. The *construction* of a minimal solution to (1) seems to depend somehow on the simple continued fraction expansion of $\sqrt{b/a}$ (or equivalently, of $\sqrt{a/b}$). It is however *false*, in general, that for any solution (x, y) of (1), x/y is a convergent of the simple continued fraction expansion for $\sqrt{b/a}$. Nevertheless, a finite algorithm exists for finding the minimal solution (x_0, y_0), if any, of (1). By solving the congruence

$$-by^2 \equiv c \pmod{a} \tag{4}$$

implied by (3), and also using the inequality

$$0 < y_0 < \sqrt{cu_1/2b}, \tag{5}$$

where (u_1, v_1) is the minimal *nontrivial* solution of the auxiliary equation

$$u^2 - abv^2 = 1, \tag{6}$$

[the trivial one is $(u_0, v_0) = (1, 0)$], we may determine in a finite number of trials if a solution exists. It would be far more desirable, however, to construct such a minimal solution of (1) *directly*, rather than by trial and error.

III. Given that (x_0, y_0) is the minimal solution of (1), and (u_n, v_n) the solutions of the auxiliary equation in (6) (which latter solutions are known to exist in all cases, and for which several constructive algorithms are known), then *all* solutions of (1) are given by:

$$x_n = x_0u_n + by_0v_n, \quad y_n = y_0u_n + ax_0v_n, \quad n \in \mathbb{Z}. \tag{7}$$

Note that the solutions (u_n, v_n) of (6) are given by:

$$u_n = \frac{1}{2}(p^n + q^n), \quad v_n = \frac{1}{2\sqrt{ab}}(p^n - q^n), \quad n \in \mathbb{Z}, \tag{8}$$

where

$$p = u_1 + v_1\sqrt{ab}, \quad q = u_1 - v_1\sqrt{ab}. \tag{9}$$

IV. We note that $u_{-n} = u_n$, $v_{-n} = -v_n$ for all $n \in \mathbb{Z}$. From this it may be deduced that $x_n > 0$ for all n, while y_n has the same sign as n. This eliminates trivial variations in solutions due to sign, and makes the theory more elegant.

* * *

Correction to H-382

The left-hand side of (3) should read F_{n+2}, and the left-hand side of (4) should read F_{n+2}.

Correction to H-381

Equation (ii) should read

$$\text{(ii)} \qquad \beta(2m-1) = \sum_{i=1}^{m-1} \frac{(-)^{i+1}u^{2i}}{2^{2i}(2i)!}\,\beta(2m-2i-1), \quad m \geqslant 2.$$

Ring around the Lucas!

H-362 *Proposed by Stanley Rabinowitz, Merrimack, NH*
(Vol. 21, no. 4, November 1983)

Let Z_n be the ring of integers modulo n. A *Lucas number* in this ring is a member of the sequence $\{L_k\}$, $k = 0, 1, 2, \ldots$, where

$$L_0 = 2,\ L_1 = 1, \text{ and } L_{k+2} \equiv L_{k+1} + L_k \text{ for } k \geqslant 0.$$

Prove that for $n > 14$, all members of Z_n are Lucas numbers if and only if n is a power of 3.

Remark: A similar, but more complicated, result is known for Fibonacci numbers. See [1]. I do not have a proof of the above proposal, but I suspect a proof similar to the result in [1] is possible; however, it should be considerably simpler because there is only one case to consider rather than seven cases.

To verify the conjecture, I ran a computer program that examined Z_n for all n between 2 and 10,000 and found that the only cases where all members of Z_n were Lucas numbers were powers of 3 and the exceptional values $n = 2, 4, 6, 7,$ and 14 (the same exceptions found in [1]). This is strong evidence for the truth of the conjecture.

Reference

1. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *The Fibonacci Quarterly* 9, no. 5 (1971):497.

Solution by Paul S. Bruckman, Fair Oaks, CA

We generalize and modify the definition of *defectiveness* indicated in [1]. Given a positive integer n, let $R_n = \{0, 1, 2, \ldots, n-1\}$ denote a complete residue class (mod n), and consider the (periodic) sequence

$$(L_r \pmod n)_{r=0}^{\infty} = (L_r')_{r=0}^{\infty}$$

with elements in R_n. Let $k = k(n)$ denote the period of this sequence. We say n is *Lucas-defective* if $R_n \not\subset \{L_0', L_1', L_2', \ldots, L_k'\}$, i.e., if there exists $j \in R_n$ such that $L_i \not\equiv j \pmod n$ for all $i \geqslant 0$. Let *LD* denote the set of all Lucas-defective numbers. A comparable definition using Fibonacci numbers instead of Lucas numbers may be made, with *FD* denoting the comparable set of *Fibonacci-defective* numbers; these were simply called *defective* numbers in Burr's paper [1]. Let *LD** and *FD** denote the complements of *LD* and *FD*, respectively, with respect to $\mathbb{N} = \{1, 2, 3, \ldots\}$, i.e.,

$$LD^* = \mathbb{N} - LD, \quad FD^* = \mathbb{N} - FD.$$

We recall the main result of Burr:

Theorem 1

FD^* consists of the following numbers:

$$5^u, \quad 2 \cdot 5^u, \quad 4 \cdot 5^u, \quad 6 \cdot 5^u, \quad 7 \cdot 5^u, \quad 14 \cdot 5^u, \quad 3^v \cdot 5^u, \quad u \geq 0, \quad v \geq 1.$$

We will establish Rabinowitz' conjecture, namely:

Theorem 2

LD^* consists of the following numbers:

$$1, 2, 4, 6, 7, 14, 3^v, \quad v \geq 1.$$

Note that 1 is (trivially) LD^*, as well as FD^*, although Rabinowitz did not specifically mention this. We will require some preliminary lemmas.

Lemma 1

If $n \in LD$, then $kn \in LD$ for all $k \in \mathbb{N}$.

Proof of Lemma 1: Since $n \in LD$, there exists an integer $j \in R$ such that $L_i \not\equiv j \pmod{n}$ for all $i \geq 0$. Therefore, $L_i \not\equiv j \pmod{kn}$ for all $k \in \mathbb{N}$ and for all $i \geq 0$. Hence, $kn \in LD$ for all $k \in \mathbb{N}$.

Lemma 2

(a) $1, 2, 4, 6, 7, 14 \in LD^*$;

(b) $5 \in LD$.

Proof of Lemma 2: This follows from a simple, but trite, tabulation of the residues of the sequences $(L_r \pmod{n})_{r=0}^{k-1}$ for the various stated values of n, leading to the indicated results by inspection.

Note that Lemma 1 and Lemma 2(b) imply that no multiple of 5 can be in LD^*.

Lemma 3

$LD^* \subset FD^*$.

Proof of Lemma 3: Suppose $n \in LD^*$. Then there exists $j \in R_n$ such that $L_j \equiv 0 \pmod{n}$. Since $\gcd(L_j, L_{j+1}) = 1$, we have $\gcd(n, L_{j+1}) = 1$; hence, $L_{j+1}^{-1} \pmod{n}$ exists. Define the sequence $\theta_r \equiv L_{j+1}^{-1} \cdot L_r \pmod{n}$, $r = 0, 1, 2, \ldots$. Note that the θ_r's are equal to a constant integer $(L_{j+1}^{-1} \pmod{n})$ times the L_r's $(\mathrm{mod}\ n)$, and therefore satisfy the basic Fibonacci recursion. Moreover, $\theta_j \equiv 0$, $\theta_{j+1} \equiv 1 \pmod{n}$, which are the initial values of the standard Fibonacci sequence. Hence, $(\theta_r)_{r=0}^{\infty}$ is the Fibonacci sequence $(\mathrm{mod}\ n)$, except in a cyclically permuted order. Since $n \in LD^*$, the sequence of L_r's contains R_n in some order. Since $\gcd(L_{j+1}^{-1} \pmod{n}, n) = 1$, we see that multiplying the elements of R_n throughout by $L_{j+1}^{-1} \pmod{n}$ regenerates R_n in some permuted order. Hence, $(F_r \pmod{n})_{r=0}^{\infty}$ contains R_n, i.e., $n \in FD^*$. Thus, $LD^* \subset FD^*$. Combining the results of Lemmas 1, 2, and 3, we see that LD^* consists of all the numbers in

*FD** (as stated in Theorem 1), *except* all multiples of 5, and *possibly* further excepting powers of 3. It therefore suffices to prove one more result, namely:

Lemma 4

$3^v \in LD^*, \quad v \in \mathbb{N}$.

Proof of Lemma 4: Given $v \in \mathbb{N}$, let $m = 3^{v-1}$. We indicate the main result of [3] below:

$$\alpha^{3m} \equiv \beta^m, \quad \beta^{3m} \equiv \alpha^m \pmod{3m}. \tag{*}$$

This is an instance of an identity in the "calculus of complex residues" explained in [3], whereby we may manipulate the quantities $\alpha \equiv \frac{1}{2}(1 + \sqrt{5})$ and $\beta = \frac{1}{2}(1 - \sqrt{5}) \pmod{3m}$ as we would ordinarily manipulate complex numbers; in this case, however, the object $\sqrt{5}$ (rather than $\sqrt{-1}$) is "imaginary," since 5 is a quadratic nonresidue of $3m$. Note that (*) implies $\alpha^{2m} \equiv -\beta^{2m} \pmod{3m}$, i.e., $L_{2m} \equiv 0 \pmod{3m}$. Also, we have

$$\alpha^{2m+1} \equiv \beta^{2m-1}, \quad \beta^{2m+1} \equiv \alpha^{2m-1} \pmod{3m},$$

which implies $F_{2m+1} \equiv -F_{2m-1} \pmod{3m}$. Therefore, $F_{2m+1} \equiv F_{2m} - F_{2m+1} \pmod{3m}$, or

$$F_{2m} \equiv 2F_{2m+1} \pmod{3m}. \tag{**}$$

Since $\gcd(F_r, F_{r+1}) = 1$ for all r, we must therefore have $\gcd(F_{2m}, 3m) = 1$; hence, $F_{2m}^{-1} \pmod{3m}$ exists. The rest of the proof is similar to that of Lemma 3. Define the sequence $\Psi_r \equiv 2F_{2m}^{-1}F_r \pmod{3m}$, $r = 0, 1, 2, \ldots$. Then the Ψ_r's satisfy the Fibonacci recursion. Moreover, $\Psi_{2m} \equiv 2$ and $\Psi_{2m+1} \equiv 1 \pmod{3m}$, using (**); these are the initial values of the Lucas sequence. Thus, $(\Psi_r)_{r=0}^{\infty}$ is the Lucas sequence (mod $3m$), except in a cyclically permuted order. From Theorem 1, $3m \in FD^*$; hence, the sequence $(F_r \pmod{3m})_{r=0}^{\infty}$ contains R_{3m} in some permuted order. Since $\gcd(2F_{2m}^{-1} \pmod{3m}, 3m) = 1$, multiplying the elements of R_{3m} throughout by $2F_{2m}^{-1} \pmod{3m}$ regenerates R_{3m} in some permuted order; hence, $3m \in LD^*$. Q.E.D.

This completes the proof of Theorem 2 (Rabinowitz' Conjecture).

References

1. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *The Fibonacci Quarterly* 9, no. 5 (1971):497-504.
2. A. P. Shah. "Fibonacci Sequence Modulo m." *The Fibonacci Quarterly* 6, no. 2 (1968):139-41.
3. P. S. Bruckman. "Some Divisibility Properties of Generalized Fibonacci Sequences." *The Fibonacci Quarterly* 17, no. 1 (1979):42-49.

Also solved by L. Somer.

◆◇◆◇◆