ADVANCED PROBLEMS AND SOLUTIONS

Edited by
Raymond E. Whitney

Please send all communications 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-452 *Proposed by Don Redmond, Southern Illinois U., Carbondale, IL*

Let $p_r(m)$ denote the m^{th} r-gonal number $(m/2)\{2 + (r-2)(m-1)\}$. Characterize the values of r and m such that

$$p_r(m) \,\Big|\, \sum_{k=1}^{m} p_r(k).$$

H-453 *Proposed by James E. Desmond, Pensacola Jr. College, Pensacola, FL*

Show that for positive integers m and n,

$$\frac{L_{(2m+1)n}}{L_n} = \sum_{j=1}^{m} (-1)^{(n+1)(m-j)} L_{2nj} + (-1)^{m(n+1)}$$

and

$$\frac{F_{2mn}}{L_n} = \sum_{j=1}^{m} (-1)^{(n+1)(m-j)} F_{n(2j-1)}.$$

H-454 *Proposed by Larry Taylor, Rego Park, NY*

Construct six distinct Fibonacci-Lucas identities such that

(a) Each identity consists of three terms;
(b) Each term is the product of two Fibonacci numbers;
(c) Each subscript is either a Fibonacci or a Lucas number.

SOLUTIONS

An Old-Timer

H-91 *Proposed by Douglas Lind, U. of Virginia, Charlottesville, VA (Vol. 4, no. 3, October 1966) [corrected]*

Let $m = \left[\frac{k}{2}\right]$, then show

$$\frac{F_{kn}}{F_n} = \sum_{j=0}^{m-1} (-1)^{jn} L_{n(k-1-2j)} + e_n,$$

where

$$e_n = \begin{cases} (-1)^{mn} & \text{if } k \text{ is odd} \\ 0 & \text{if } k \text{ is even} \end{cases}$$

and $[x]$ is the greatest integer not exceeding x.

Solution by James E. Desmond, Pensacola Jr. College, Pensacola, FL

Using the well-known algebraic identity,

$$\frac{x^k - y^k}{x - y} = \sum_{j=0}^{\left[\frac{k}{2}\right]-1} x^j y^j (x^{k-1-2j} + y^{k-1-2j}) + x^{\left[\frac{k}{2}\right]} y^{\left[\frac{k}{2}\right]} \frac{1 + (-1)^{k+1}}{2}$$

for all positive integers k and nonzero real numbers x, y with $x \neq y$; let $x = \alpha^n$ and $y = \beta^n$ where n is a positive integer. We obtain

$$\frac{\alpha^{nk} - \beta^{nk}}{\alpha^n - \beta^n} = \sum_{j=0}^{\left[\frac{k}{2}\right]-1} \alpha^{nj} \beta^{nj} (\alpha^{n(k-1-2j)} + \beta^{n(k-1-2j)}) + \alpha^{n\left[\frac{k}{2}\right]} \beta^{n\left[\frac{k}{2}\right]} \frac{1 + (-1)^{k+1}}{2}.$$

That is,

$$\frac{F_{nk}}{F_n} = \sum_{j=0}^{\left[\frac{k}{2}\right]-1} (-1)^{nj} L_{n(k-1-2j)} + (-1)^{n\left[\frac{k}{2}\right]} \frac{1 + (-1)^{k+1}}{2}$$

$$= \sum_{j=0}^{m-1} (-1)^{jn} L_{n(k-1-2j)} + e_n.$$

Pell-Mell

<u>H-433</u> *Proposed by H.-J. Seiffert, Berlin, Germany (Vol. 27, no. 4, August 1989)*

Let $P_0, P_1, \ldots$ be the Pell numbers defined by

$$P_0 = 0,\ P_1 = 1,\ P_n = 2P_{n-1} + P_{n-2} \text{ for } n \geq 2.$$

Show that, for $n = 1, 2, \ldots,$

$$6(n + 1)P_{n-1} + P_{n+1} \equiv (-1)^{n+1}(9n^2 - 7)F_{n+1} \pmod{27}.$$

Solution by Robert B. Israel, U. of British Columbia, Vancouver, B.C.

The congruence

(1) $\quad P_n \equiv (-1)^n((18n^2 + 21n + 2)F_n + 12nF_{n+1}) \pmod{27}$, for all $n \geq 0$,

can be established by checking that the right-hand side obeys the defining equations for P_n mod 27. Some tedious but straightforward manipulations then lead to the desired result.

Not content to let the matter rest there, we generalize it. Let p and k be natural numbers, and define U_n by

$$U_0 = 0,\ U_1 = 1,\ U_n = (p - 1)U_{n-1} + U_{n-2}$$

(so that the Pell numbers are the case $p = 3$).

Theorem: If no prime factors of p are equal to 5 or less than k, there is a congruence

$$(2)\qquad U_n \equiv (-1)^n \sum_{j=0}^{k-1} n^j (a_j F_n + b_j F_{n+1}) \pmod{p^k}, \text{ for all } n \geq 0,$$

where a_j and b_j are integers.

It is more convenient to work with $V_n = (-1)^{n+1} U_n$. The generating functions of F_n and V_n are, respectively,

$$F(z) = \frac{z}{1 - z - z^2} \quad\text{and}\quad V(z) = \frac{z}{1 + (p-1)z - z^2}.$$

Letting $x = z^{-1} - 1 - z$, we have $F(z) = x^{-1}$ and

$$V(z) = \frac{1}{x + p} \equiv \sum_{j=0}^{k-1} (-p)^j x^{-1-j} \pmod{p^k}$$

(this being interpreted as a statement about formal power series in the indeterminate z with coefficients in the integers mod p^k). The generating function of $n^j F_n$ is

$$G_j(z) = \left(z\frac{d}{dz}\right)^j F(z).$$

The generating function of $(n+1)^j F_{n+1}$ is $z^{-1} G_j(z)$. To prove the theorem, it is enough to prove that for $2 \leq j \leq k$ there are congruences

$$(3)\qquad x^{-j} \equiv \sum_{i=0}^{j-1} (c_i + d_i z^{-1}) G_i(z) \pmod{p^k}.$$

Let $w = z^{-1} + z$. I claim that

$$(4)\qquad G_{2j}(z) = \sum_{i=1}^{2j+1} \frac{c_{i,2j}}{x^i} \quad\text{with } c_{2j+1,2j} = (2j)!5^j,$$

$$(5)\qquad G_{2j+1}(z) = \sum_{i=2}^{2j+2} c_{i,2j+1} \frac{w}{x^i} \quad\text{with } c_{2j+2,2j} = (2j+1)!5^j,$$

where $c_{i,j}$ are integers. The proof is by induction, using the identities

$$z\frac{dx}{dz} = -w, \quad z\frac{dw}{dz} = -x - 1, \quad w^2 = (x+1)^2 + 4 = 5 + 2x + x^2.$$

Equation (4) allows us to express $1/x^{2j+1}$ mod p^k in terms of $G_{2j}(z)$ and lower powers of $1/x$, as long as $(2j)!5^j$ is invertible mod p^k. To treat $1/x^{2j+2}$ similarly, we first use the identity $(2z^{-1} - 1)w = (2z^{-1} + 1)x + 5$ and (5) to get

$$(6)\qquad \frac{(2j+1)!5^{j+1}}{x^{2j+2}} = (2z^{-1} - 1)G_{2j+1} - \sum_{i=1}^{2j+1} \frac{5c_{i,2j+1} + c_{i+1,2j+1}}{x^i} - 2\sum_{i=1}^{2j+1} c_{i+1,2j+1} \frac{z^{-1}}{x^i},$$

where $c_{1,2j+1} = 0$. The factors of z^{-1} that arise here are harmless. To avoid factors of z^{-2}, however, we can use the identity $(z^{-1} + 2)w = (z^{-1} - 2)x + 5z^{-1}$ together with (5) to get

$$\frac{(2j+1)!5^{j+1}z^{-1}}{x^{2j+2}} = (z^{-1} + 2)G_{2j+1} - \sum_{i=1}^{2j+1} (5c_{i,2j+1} + c_{i+1,2j+1})\frac{z^{-1}}{x^i} + 2\sum_{i=1}^{2j+1} \frac{c_{i+1,2j+1}}{x^i}.$$

Repeated use of these formulas results in the desired congruences (3).

In the case $k = 3$, for example, the result of all of this is

$$U_n \equiv (-1)^n\left(\left(-\frac{p^2n^2}{10} - \frac{3p^2n}{50} - \frac{pn}{5} + \frac{p^2}{25} - \frac{p}{5} - 1\right)F_n + \left(\frac{3p^2n}{25} + \frac{2pn}{5}\right)F_{n+1}\right) \pmod{p^3}$$

if $(p, 10) = 1$. With $p = 3$, this yields (1).

Also solved by P. Bruckman, R. J. Hendel, L. Kuipers, G. Wulczyn, and the proposer.

Strange Sex

H-434 *Proposed by Piero Filipponi & Odoardo Brugia, Rome, Italy (Vol. 27, no. 4, August 1989)*

Strange creatures live on a planet orbiting around a star in a remote galaxy. Such beings have three sexes (namely, sex A, sex B, and sex C) and are reproduced as follows:

(i) An individual of sex A (or simply A) generates individuals of sex C by parthenogenesis.

(ii) If A is fertilized by an individual of sex B, then A generates individuals of sex B.

(iii) In order to generate individuals of sex A, A must be fertilized by an individual of sex A, an individual of sex B, and an individual of sex C.

Find a closed form expression for the number T_n of ancestors of an individual of sex A in the n^{th} generation. Note that, according to (i), (ii), and (iii), A has three parents ($T_1 = 3$) and six grandparents ($T_2 = 6$).

Solution by Russell Jay Hendel, Dowling College, Oakdale, NY

We claim

$$T_n = c_1\left[r_1^n + \frac{1}{2}\right], \quad \text{for all } n \ge 0;$$

with $r_1 \ge r_2 \ge 0 \ge r_3$ the three roots of $p(z) = z^3 - 2z^2 - z + 1$; and

$$c_1 = \frac{r_1^2 + r_1 - 1}{(r_2 - r_1)(r_3 - r_1)} \approx 1.22144\ldots .$$

The proof will use complex variable methods to derive the value of the c_i and linear algebra methods to derive the value of T_n.

First, define a homomorphism, H, on the free monoid on the letters {A, B, C} by $H(\text{C}) = \text{A}$, $H(\text{B}) = \text{AB}$, and $H(\text{A}) = \text{ABC}$, so that T_n equals the length of the string $P^n(\text{A})$. Following Rauzy [2], a convenient way to study this length is by letting M be the 3×3, 1-0, upper triangular matrix, defined by $M(i, j) = 1$ if $i + j \ge 4$, and 0 otherwise.

Following Rorres & Anton [3], define vectors

$$\mathbf{v}_{-1} = (1, 0, 0)^* \quad \text{and} \quad M\mathbf{v}_{n-1} = \mathbf{v}_n = (x_n, y_n, z_n)^*,$$

with * denoting vector transpose. Thus, $x_n = T_n$, and

$$\mathbf{v}_n = M^{n+1}\mathbf{v}_{-1} = PD^{n+1}P^{-1}\mathbf{v}^{-1},$$

with $M = PDP^{-1}$, a diagonal decomposition of M. Since the characteristic polynomial of M is $p(z)$, some straightforward manipulation yields

$$x_n = \sum_{i=1}^{3} c_i r_i^n,$$

for some constants c_i, $1 \le i \le 3$.

To find closed formulas for the c_i, we study the generating function

$$T(z) = \sum_{i=0}^{\infty} T_i z^i = \frac{1 + z - z^2}{z^3 p(z^{-1})} = \frac{1 + z - z^2}{\prod_{i=1}^{3}(z - r^{-1})}.$$

Following Hagis [1], we employ the Residue Theorem to yield:

$$\frac{1}{2\pi i}\int_{C_s} \frac{T(z)}{z^{n+1}}\,dz = \frac{1}{2\pi i}\int_{C_0} \frac{T(z)}{z^{n+1}}\,dz + \frac{1}{2\pi i}\sum_{i=1}^{3}\int_{C_i} \frac{T(z)}{z^{n+1}}\,dz$$

where C_S is the circle of radius S about the origin, and C_0 and C_i are circles of radius .1 around the origin and the r_i^{-1}, respectively. By the triangle inequality for integrals, as S goes to infinity we have

$$\left|\frac{1}{2\pi i}\int_{C_s} \frac{T(z)}{z^{n+1}}\,dz\right| \le O(S^{-1}) \to 0.$$

By the Cauchy Integral Formula for derivatives, we have

$$\frac{1}{2\pi i}\int_{C_0} \frac{T(z)}{z^{n+1}}\,dz = \frac{T^{(n)}(0)}{n!} = T_n.$$

Finally, by the Cauchy Integral Formula and some manipulations, we have

$$\frac{1}{2\pi i}\int_{C_i} \frac{T(z)}{z^{n+1}}\,dz = \text{Residue at } r_i^{-1} = \frac{r_i^2 + r_i - 1}{\prod_{j \ne i}(r_j - r_i)}\, r_i^n.$$

Combining the above, we have an alternate derivation of the preliminary formula for the T_n with closed expression for the c_i.

To complete the proof, simply observe that, for large n,

$$T_n - c_1 r_1^n = c_2 r_2^n + c_3 r_3^n = O(|r_3|)^n \to 0.$$

For small n, a calculator can be used to verify that an upper bound for the absolute value of the preceding expression is bounded by 1/2. The details are left to the reader. (In passing, we note that it is straightforward to prove that $T_n - c_1 r_1^n$ is oscillating and monotone in opposite directions for even and odd n.)

References

1. P. Hagis. "An Analytic Proof of the Formula for F_n." *Fibonacci Quarterly 2* (1964):267-68.
2. Rauzy. "Nombres algebriques et substitutions." *Bull. Soc. Math. France 110* (1982):147-78.
3. C. Rorres & H. Anton. *Applications of Linear Algebra*. New York: Wiley, 1984.

Probably

H-436 *Proposed by Piero Filipponi, Rome, Italy*
(Vol. 27, no. 5, November 1989)

For p an arbitrary prime number, it is known that

$$(p - 1)! \equiv p - 1 \pmod p, \quad (p - 2)! \equiv 1 \pmod p,$$

and

$$(p - 3)! \equiv (p - 1)/2 \pmod p.$$

Let k_0 be the smallest value of an integer k for which $k! > p$.

The numerical evidence turning out from computer experiments suggests that the probability that, for k varying within the interval $[k_0, p - 3]$, $k!$ reduced modulo p is either even or odd is 1/2. Can this conjecture be proved?

Solution by Paul S. Bruckman, Edmonds, WA

We will show that the proposer's conjecture is equivalent to the proposition that the primes are somehow equally distributed, a concept which we will define more precisely later. First, we form the following short table of $k_0 = k_0(p)$, for the first few primes p:

p	k_0
2	3
3	3
5	3
7	4
11	4

Clearly, $k_0 \le p - 3$ only if $p \ge 7$; suppose then that $p \ge 7$ henceforth. Now any such prime must be of one of the two forms: $4a + 1$ or $4a + 3$. Then

$$(p - 3)! \equiv \frac{1}{2}(p - 1) \equiv 2a \text{ or } 2a + 1.$$

Note that these are *proper* residues (mod p), that is, lie in the interval $[1, p - 1]$. We introduce the notation: $\overline{f(p) \equiv x}$ to mean that $f(p) \equiv x \pmod p$, and $x \in [1, p - 1]$. If we can expect that a prime is equally likely to be of either form, it would then follow that $\Pr[\overline{(p - 3)!}$ is even$] = 1/2$. This seems a plausible supposition, but is apparently an unproven proposition.

We now tackle the general case. Consider $(p - r - 1)!$, where r is chosen so that $r \in [2, p - 1 - k_0]$. Then

$$\begin{aligned}(p - r - 1)! &= (p - 2)!/(p - 2)(p - 3) \ldots (p - r)\\ &\equiv 1/(-1)^{r-1}2 \cdot 3 \cdot \cdots \cdot r,\end{aligned}$$

or

(1) $$(p - r - 1)! \equiv (-1)^{r-1}(r!)^{-1} \pmod p.$$

Since g.c.d.$(p, r!) = 1$, there exists some integer b such that

(2) $$p \equiv b \pmod{2(r!)}.$$

As b assumes all values in $[1, 2(r!) - 1]$ with g.c.d.$(b, r!) = 1$, it is clear that any prime p must be of one of those forms [there are $2\phi(r)$ such, where ϕ is the Euler (totient) function]. Again, we may reasonably conjecture that each choice of b is equally probable, as p is randomly chosen. For example, for $r = 3$, there are $2\phi(3) = 4$ choices: $p \equiv 1, 5, 7$, or $11 \pmod{12}$, and we may plausibly suppose that each form of p is equally likely.

Now, there are infinitely many integers x such that congruence $px \equiv (-1)^r \pmod{r!}$ has solutions. However, if we restrict x to the interval $(0, r!)$, then $x = c$ is uniquely determined. Hence,

$$(cp - (-1)^r)/r! \equiv (-1)^{r-1}(r!)^{-1} \pmod p;$$

therefore, from (1), we have:

(3) $$(p - r - 1)! \equiv (cp - (-1)^r)/r! \pmod p.$$

Moreover,

$$(cp - (-1)^r)/r! \geq (p - 1)/r! \geq \frac{2(r!) + 1 - 1}{r!} \geq 2,$$

and

$$(cp - (-1)^r)/r! \leq \frac{(r! - 1)p + 1}{r!} = p - (p - 1)/r!$$

$$\leq p - (2(r!) + 1 - 1)/r! = p - 2.$$

This shows that $(cp - (-1)^r)/r!$ is a proper residue (mod p). We have proven the following result.

Lemma 1:

(4) $\qquad \underline{(p - r - 1)!} \equiv (cp - (-1)^r)/r!,\ r = 2, 3, \ldots, p - 1 - k_0,$

where c is uniquely determined by $c \equiv (-1)^r p^{-1}$ (mod $r!$), $0 < c < r!$.

Now, given r, suppose we choose b such that $0 < b < r!$, and that $p \equiv b$ (mod $2(r!)$), for some prime p. Also suppose that p' is prime, where $p' \equiv b'$ (mod $2(r!)$), and $b' = b + r!$ [hence, $r! < b' < 2(r!)$ and g.c.d.$(b', r!) = 1$). Let c and c' denote the values determined from Lemma 1, with p and p', respectively. Thus, $p = 2a(r!) + b$, $p' = 2a'(r!) + b'$ for some integers a and a'. From Lemma 1,

$$c \equiv (-1)^r p^{-1} \equiv (-1)^r/[2a(r!) + b] \equiv (-1)^r b^{-1} \pmod{r!};$$

also,

$$c' \equiv (-1)^r (p')^{-1} \equiv (-1)^r/[2a'(r!) + b + r!] \equiv (-1)^r b^{-1} \pmod{r!}.$$

Hence, $c' \equiv c$ (mod $r!$). However, since $0 < c < r!$ and $0 < c' < r!$, it follows that $c' = c$. Also, from Lemma 1,

$$\underline{(p' - r - 1)!} \equiv [cp' - (-1)^r]/r! = \frac{c[2a'(r!) + b + r!] - (-1)^r}{r!}$$

$$= \frac{c[2a(r!) + b] + (2a' - 2a)cr! - (-1)^r}{r!} + c$$

$$= [cp - (-1)^r]/r! + (2a' - 2a + 1)c.$$

Note that c must be an odd number, since $r!$ is even and $r!$ divides $(cp - (-1)^r)$. Hence, we have proven the following result.

Lemma 2: Given primes p and p',

$$2 \leq r \leq \min\{(p - 1 - k_0),\ (p' - 1 - k_0')\},$$

where $k_0' = k_0(p')$ and $p' \equiv p + r!$ (mod $2(r!)$), then $\underline{(p' - r - 1)!}$ and $\underline{(p - r - 1)!}$ are disparate.

If it is true that each prime p of the form $p \equiv b$ (mod $2(r!)$) is equally likely, as b varies over its $2\phi(r!)$ possible values, then it would follow from Lemma 2 that Prob[$\underline{(p - r - 1)!}$ is even] = 1/2. Letting r vary over its possible values $r = \overline{2, 3, \ldots, p - 1} - k_0$, we could then conclude that

$$\text{Prob}(\underline{k!} \text{ is even}) = \frac{1}{2}, \text{ for } k = k_0, k_0 + 1, \ldots, p - 3,$$

where p is a random prime. Thus, given integers $r \geq 2$ and $b \in [1, 2(r!) - 1]$, with g.c.d.$(b, r!) = 1$, the following results are equivalent, for random primes p:

(a) Prob($p \equiv b$ (mod $2(r!)$)) = $1/2\phi(r!)$;

(b) Prob[$\underline{(p - r - 1)!}$ is even] = $\frac{1}{2}$.

The result conjectured in (a) seems plausible enough; however, as far as is known, it remains unproven.

*****