ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY
Lock Haven State College, Lock Haven, PA 17745

Send all communications concerning ADVANDED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, MATHEMATICS DEPARTMENT, LOCK HAVEN STATE COLLEGE, 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, solutions should be submitted on separate, signed sheets within two months after publication of the problems.

PROBLEMS

H-342 *Proposed by Paul S. Bruckman, Concord, CA*

Let

(1) $$A_n = \sum_{k=0}^{[\frac{1}{2}n]} \binom{n}{k}\binom{2n-2k}{n}4^k, \quad n = 0, 1, 2, \ldots .$$

Prove that

(2) $$\sum_{k=0}^{n} A_k A_{n-k} = 4^n F_{n+1}.$$

H-343 *Proposed by Verner E. Hoggatt, Jr., deceased*

Show that every positive integer m has a unique representation in the form

$$m = [A_1[A_2[A_3[\ldots[A_n]\ldots],$$

where $A_j = \alpha$ or α^2 for $j = 1, 2, \ldots, n-1$, and

$$A_n = \alpha^2, \text{ where } \alpha = (1+\sqrt{5})/2.$$

H-344 *Proposed by M. D. Agrawal, Government College, Mandasaur, India*

Prove:

1. $L_k L_{k+3m}^2 - L_{k+4m} L_{k+m}^2 = (-1)^k 5^2 F_m^2 F_{2m} F_{k+2m}$, and
2. $L_k L_{k+3m}^2 - L_{k+2m}^3 = 5(-1)^k F_m^2 (L_{k+4m} + 2(-1)^m L_{k+2m})$.

SOLUTIONS

Say A

(Corrected)
H-324 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA (Vol. 19, No. 1, February 1981)*

Establish the identity

$$A \equiv F_{14r}(F^7_{n+4r} + F^7_n) - 7F_{10r}(F^6_{n+4r}F_n + F_{n+4r}F^6_n) + 21F_{6r}(F^5_{n+4r}F^2_n + F^2_{n+4r}F^5_n) - 35F_{2r}(F^4_{n+4r}F^3_n + F^3_{n+4r}F^4_n)$$

$$= F^7_{4r}F_{7n+14}.$$

Solution by Paul S. Bruckman, Concord, CA

We first observe that there is a misprint in the statement of the problem. The first quantity under the first parenthesis in the definition of A should be "F^7_{n+4r}," not "F^7_{n+14r}." For brevity, let

(1) $$u = F_{n+4r},\ v = F_n.$$

Using the extension to negative integers:

(2) $$F_{-m} = (-1)^{m-1}F_m,$$

we see that we may express A as follows:

$$A = \sum_{k=0}^{7}\binom{7}{k}u^{7-k}(-v)^kF_{(14-4k)r}.$$

Thus,

$$A\sqrt{5} = \sum_{k=0}^{7}\binom{7}{k}u^{7-k}(-v)^k\{a^{14r-4kr} - b^{14r-4kr}\},$$

where $a = \frac{1}{2}(1 + \sqrt{5})$, $b = \frac{1}{2}(1 - \sqrt{5})$; thus

$$A\sqrt{5} = a^{14r}\sum_{k=0}^{7}\binom{7}{k}u^{7-k}(-va^{-4r})^k - b^{14r}\sum_{k=0}^{7}\binom{7}{k}u^{7-k}(-vb^{-4r})^k$$

$$= a^{14r}(u - vb^{4r})^7 - b^{14r}(u - va^{4r})^7, \text{ or}$$

(3) $$A\sqrt{5} = (ua^{2r} - vb^{2r})^7 - (ub^{2r} - va^{2r})^7.$$

Now

$$ua^{2r} - vb^{2r} = 5^{-1/2}\{a^{2r}(a^{n+4r} - b^{n+4r}) - b^{2r}(a^n - b^n)\}$$

$$= 5^{-1/2}(a^{n+6r} - b^{n+2r} - a^nb^{2r} + b^{n+2r})$$

$$= 5^{-1/2}a^{n+2r}(a^{4r} - b^{4r}) = a^{n+2r}F_{4r}.$$

Also,

$$ub^{2r} - va^{2r} = 5^{-1/2}\{b^{2r}(a^{n+4r} - b^{n+4r}) - a^{2r}(a^n - b^n)\}$$

$$= 5^{-1/2}(a^{n+2r} - b^{n+6r} - a^{n+2r} + a^{2r}b^n) = 5^{-1/2}b^{n+2r}(a^{4r} - b^{4r}) = b^{n+2r}F_{4r}.$$

Therefore, $A\sqrt{5} = (a^{n+2r}F_{4r})^7 - (b^{n+2r}F_{4r})^7 = (a^{7n+14r} - b^{7n+14r})F_{4r}^7$, or

(4) $$A = F_{4r}^7 F_{7n+14r}. \qquad \text{Q.E.D.}$$

Also solved by the proposer.

Sum Fun

H-325 *Proposed by Leonard Carlitz, Duke University, Durham NC (Vol. 19, No. 1, February 1981)*

For arbitrary a, b put

$$S_m(a, b) = \sum_{j+k=m} \binom{a}{j}\binom{b+k-1}{k} \qquad (m = 0, 1, 2, \ldots).$$

Show that

(1) $$\sum_{m+n=p} S_m(a, b)S_n(c, d) = S_p(a+c, b+d)$$

(2) $$\sum_{m+n=p} (-1)^n S_m(a, b)S_n(c, d) = S_p(a-d, b-c).$$

Solution by the proposer.

We have

(3) $$\sum_{m=0}^{\infty} S_m(a, b)x^m = \sum_{j,k=0}^{\infty} \binom{a}{j}\binom{b+k-1}{k}x^{j+k} = (1+x)^a(1-x)^{-b}.$$

Thus

$$\begin{aligned}\sum_{p=0}^{\infty} x^p \sum_{m+n=p} S_m(a, b)S_n(c, d) &= \sum_{m=0}^{\infty} S_m(a, b)x^m \sum_{n=0}^{\infty} S_n(c, d)x^n \\ &= (1+x)^a(1-x)^{-b}(1+x)^c(1-x)^{-d} \\ &= (1+x)^{a+c}(1-x)^{-b-d} \\ &= \sum_{p=0}^{\infty} S_p(a+c, b+d)x^p.\end{aligned}$$

Equating coefficients of x^p, we get (1). By (3) we have

$$\sum_{n=0}^{\infty} (-1)^n S_n(c, d)x^n = (1-x)^c(1+x)^{-d}.$$

Hence

$$\begin{aligned}\sum_{p=0}^{\infty} x^p \sum_{m+n=p} (-1)^n S_m(a, b)S_n(c, d) &= (1+x)^a(1-x)^{-b}(1-x)^c(1+x)^{-d} \\ &= (1+x)^{a-d}(1-x)^{-(b-c)}\end{aligned}$$

and (2) follows immediately.

Also solved by P. Bruckman.

A Primitive Solution

H-326 *Proposed by Larry Taylor, Briarwood, NY (Vol. 19, No. 1, February 1981)*

(A) If $p \equiv 7$ or $31 \pmod{36}$ is prime and $(p-1)/6$ is also prime, prove that $32(1 \pm \sqrt{-3})$ is a primitive root of p.

(B) If $p \equiv 13$ or $61 \pmod{72}$ is prime and $(p-1)/12$ is also prime, prove that $32(\sqrt{-1} \pm \sqrt{3})$ is a primitive root of p.

For example, $11 \equiv \sqrt{-3} \pmod{31}$, 12 and 21 are primitive roots of 31; $11 \equiv \sqrt{-1} \pmod{61}$, $8 \equiv \sqrt{3} \pmod{61}$, 59 and 35 are primitive roots of 61.

Solution by Paul S. Bruckman, Concord, CA

Part (A): We must first show that $(-3/p) = 1$, so that we can indeed define $x \equiv 32(1 \pm \sqrt{-3}) \pmod{p}$. Since $(p/3) = (7/3) = (31/3) = 1$, thus $(3/p)(p/3) = (-1)^{1/2(p-1)} = -1$, or $(3/p) = -1$. Thus,

$$(-3/p) = (-1/p)(3/p) = (-1)^{1/2(p-1)}(3/p) = (-1)^2 = 1,$$

which shows that x exists.

Let $w \equiv 2^{-1}(1 \pm \sqrt{-3}) \pmod{p}$. Thus $x \equiv 2^6 w \pmod{p}$. Note that $p > 7$, since $q = (p-1)/6$ must be prime. Note also that $w^3 \equiv -1 \pmod{p}$. This implies that $w \not\equiv 1 \pmod{p}$. Also, $w \not\equiv -1 \pmod{p}$, for if we suppose $w \equiv -1 \pmod{p}$, then

$$1 \pm \sqrt{-3} \equiv -2 \pmod{p} \Rightarrow \pm\sqrt{-3} \equiv -3 \pmod{p} \Rightarrow -3 \equiv 9 \pmod{p} \Rightarrow p \mid 12,$$

a contradiction. We observe further that, whichever sign is taken with $\sqrt{-3}$ in the definition of w, the other sign must be taken to define w^{-1}, since

$$2^{-1}(1 + \sqrt{-3})2^{-1}(1 - \sqrt{-3}) \equiv 4^{-1} \cdot 4 \equiv 1 \pmod{p}.$$

But, since $w^3 \equiv -1 \pmod{p}$, thus $w^{-1} \equiv -w^2 \pmod{p}$. We conclude that $w \not\equiv \pm 1 \pmod{p}$ and $w^2 \not\equiv \pm 1 \pmod{p}$.

In order to show that x is a primitive root of p, it suffices to show that $x^m \not\equiv 1 \pmod{p}$ for all proper divisors m of $\varphi(p) = p - 1 = 6q$. Since all the proper divisors of $6q$ divide at least one of the exponents $6, 2q$, and $3q$, it suffices to show that x^6, x^{2q}, and x^{3q} are $\not\equiv 1 \pmod{p}$.

Now $x^6 \equiv 2^{36}w^6 \equiv 2^{36}(-1)^2 \equiv 2^{36} \pmod{p}$. Note that

$$2^{36} - 1 = 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109.$$

Since all the primes in this decomposition are $\not\equiv 7$ or $31 \pmod{36}$, with the exception of 7, which is excluded, the congruence $2^{36} \equiv 1 \pmod{p}$ is impossible. Thus $x^6 \not\equiv 1 \pmod{p}$.

Since $q = 6r \pm 1$ for some r, $w^q \equiv w^{6r \pm 1} \equiv w^{\pm 1} \equiv w$ or $-w^2 \not\equiv \pm 1 \pmod{p}$; similarly, $(w^{-1})^q \not\equiv \pm 1 \pmod{p}$. Thus, $x^q \equiv 2^{6q}w^q \equiv 2^{p-1}w^q \equiv w^q \not\equiv 1 \pmod{p}$.

Thus, $x^{2q} \equiv (w^2)^q \equiv (-w^{-1})^q \equiv -(w^{-1})^q \not\equiv 1 \pmod{p}$. Finally,

$$x^{3q} \equiv (w^3)^q \equiv (-1)^q \equiv -1 \not\equiv 1 \pmod{p}.$$

This completes the proof of (A).

Part (B): The proof of (B) is patterned after that for (A). Since

$$(p/3) = (13/3) = (61/3) = 1,$$

thus $(3/p)(p/3) = (-1)^{1/2(p-1)} = 1$, or $(3/p) = 1$. Also, $(-1/p) = (-1)^{1/2(p-1)} = 1$. Defining $y \equiv 32(\sqrt{-1} \pm \sqrt{3}) \pmod{p}$, we then see that y exists. Also, we see that $(-3/p) = 1$.

Let $\theta \equiv 2^{-1}(\sqrt{-1} \pm \sqrt{3}) \pmod{p}$. Then $y \equiv 2^6\theta \pmod{p}$. Note that $p > 13$, since $q = (p-1)/12$ must be prime. Note also that $\theta^2 \equiv 2^{-1}(1 \pm \sqrt{-3}) \pmod{p}$, and $\theta^6 \equiv -1 \pmod{p}$. This implies that θ and θ^3 are $\not\equiv \pm 1 \pmod{p}$ and $\theta^2 \not\equiv 1 \pmod{p}$. Moreover, $\theta^2 \not\equiv -1 \pmod{p}$, for the congruence $\theta^2 \equiv -1 \pmod{p}$ would, as in part (A), lead to a contradiction. Also, whichever sign is taken with $\sqrt{3}$ in the definition of θ, the other sign must be taken to define $-\theta^{-1}$, since

$$2^{-1}(\sqrt{-1} + \sqrt{3})2^{-1}(\sqrt{-1} - \sqrt{3}) \equiv 4^{-1}(-1 - 3) \equiv -1 \pmod{p}.$$

Therefore, $\theta^{-1} \not\equiv \pm 1 \pmod{p}$. Combining this with the congruences $\theta^2 \equiv -\theta^{-4} \pmod{p}$ and $\theta^3 \equiv -\theta^{-3} \pmod{p}$, we conclude that $\theta^k \not\equiv \pm 1 \pmod{p}$ if $k = \pm 1$, ± 2, ± 3, ± 4, or ± 5.

In order to show that y is a primitive root of p, it suffices to show that $y^m \not\equiv 1 \pmod{p}$ for all proper divisors m of $\varphi(p) = 12q$. Since all the proper divisors of $12q$ divide at least one of the exponents 12, $3q$, and $4q$, it suffices to show that y^{12}, y^{3q}, and y^{4q} are $\not\equiv 1 \pmod{p}$.

Now $y^{12} \equiv 2^{72}\theta^{12} \equiv 2^{72}(-1)^2 \equiv 2^{72} \pmod{p}$. We may verify that

$$2^{72} - 1 = 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 109 \cdot 241 \cdot 433 \cdot 38{,}737,$$

this being the prime decomposition. Since the only prime in this decomposition that is $\equiv 13$ or $61 \pmod{72}$ is 13, which is excluded, we see that $2^{72} \not\equiv 1 \pmod{p}$. Therefore, $y^{12} \not\equiv 1 \pmod{p}$.

Since $q = 6r \pm 1$ for some r, thus

$$y^q \equiv 2^{6q}\theta^q \equiv 2^{1/2(p-1)}\theta^{6r\pm 1} \equiv (2/p)(-1)^r\theta^{\pm 1} \equiv \pm\theta^{\pm 1} \not\equiv \pm 1 \pmod{p}.$$

Therefore,

$$y^{3q} \equiv \pm\theta^{\pm 3} \equiv \theta^{\pm 3} \not\equiv 1 \pmod{p},$$

and

$$y^{4q} \equiv \theta^{\pm 4} \not\equiv 1 \pmod{p}.$$

This completes the proof of part (B).

Also solved by the proposer.

Belated Acknowledgment

M. D. Agrawal solved H-294 and H-319.

*****