n^{th} POWER RESIDUES CONGRUENT TO ONE

M. J. DeLEON
Florida Atlantic University, Boca Raton, FL 33431
(Submitted March 1983)

It has been proved [7, Lemma 3] that an integer has the property that

$$(x,\ m) = 1 \text{ implies } x^2 \equiv 1 \pmod{m} \text{ iff } m|24.$$

To generalize this result, we make the following definition.

Definition 1

Let n be a positive integer. The integer m has *property* $P(n)$ if and only if $(x,\ m) = 1$ implies $x^n \equiv 1 \pmod{m}$.

In §1 we shall determine, for $n \geqslant 1$, all integers which have property $P(n)$; in §2 we shall prove some consequences of an integer having property $P(n)$ or a similar property.

1. INTEGERS HAVING PROPERTY $P(n)$

In Theorem 2, we shall show that the only integers having property $P(n)$, where n is an odd positive integer, are -2, -1, 1, and 2. In Theorem 3, we shall determine the integers which have property $P(n)$, where n is an even positive integer. In particular, we shall show that:

m has property $P(4)$ iff m divides $240 = 2^4 3 \cdot 5$

m has property $P(6)$ iff m divides $504 = 2^3 3^2 \cdot 7$

m has property $P(8)$ iff m divides $480 = 2^5 \cdot 3 \cdot 5$

m has property $P(10)$ iff m divides $264 = 2^3 3 \cdot 11$

m has property $P(12)$ iff m divides $65{,}520 = 2^4 3^2 5 \cdot 7 \cdot 13$

Theorem 2

Let n be an odd positive integer. The integer m has property $P(n)$ iff $m|2$.

Proof: Assume that m has property $P(n)$, where n is an odd positive integer. Thus, since $(-1,\ m) = 1$,

$$1 \equiv (-1)^n \equiv -1 \pmod{m}.$$

Therefore, $m|2$. Clearly, $m|2$ implies that m has property $P(n)$.

Theorem 3

Let n be an even positive integer and let the distinct odd primes p which are such that $\phi(p)|n$ be denoted by $p_1,\ p_2,\ \ldots,\ p_t$. Choose e such that $2^e \| n$, and for $i = 1,\ 2,\ \ldots,\ t$, choose e_i such that $\phi(p^{e_i})\ |\ n$ and $\phi(p^{e_i+1}) \nmid n$. The integer m has property $P(n)$ iff $m|2^{e+2}p_1^{e_1}p_2^{e_2}\ \ldots\ p^{e_t}$.

On page 47 of [2], it is stated that the integer

$$2^{e+2}p_1^{e_1}p_2^{e_2}\ \dots\ p^{e_t}$$

defined in Theorem 3 is the largest integer to have property $P(n)$. Given a positive integer n, Theorems 2 and 3 enable us to find all integers m that have property $P(n)$. Given an integer m, Theorem 2 of [1] and its proof enable us to find all positive integers n such that m has property $P(n)$. An earlier reference is Theorem 4-9 of [4].

We shall need the following two lemmas to prove Theorem 3.

Lemma 4

Let d, m, n be integers with n positive. If m has property $P(n)$ and $d|m$, then d has property $P(n)$.

Proof: Without loss of generality, assume $d > 1$ and $m > 1$. Let

$$m = q_1^{e_1}q_2^{e_2}\ \dots\ q_t^{e_t},$$

where $q_1, q_2, \dots, q_t$ are distinct primes and $e_1, e_2, \dots, e_t$ are positive integers. Also let $q_1, q_2, \dots, q_j$, where $1 \leqslant j \leqslant t$, be the distinct primes that divide d. We shall now prove that d has property $P(n)$. Thus, let $(a, d) = 1$. Choose b such that

$$b \equiv a \pmod{q_1^{e_1}q_2^{e_2}\ \dots\ q_j^{e_j}} \quad\text{and}\quad b \equiv 1 \pmod{q_{j+1}^{e_{j+1}}\ \dots\ q_t^{e_t}}.$$

Since $(b, m) = 1$ and m has property $P(n)$, $b^n \equiv 1 \pmod m$. Therefore, since $a \equiv b \pmod d$ and $d|m$, $a^n \equiv b^n \equiv 1 \pmod d$.

A proof of the next lemma can be found, for example, in [6, pp. 104-105].

Lemma 5

Let e be a positive integer. We have that:

(i) $a^{2^e} \equiv 1 \pmod{2^{e+2}}$ for all odd integers a.

(ii) 5 belongs to the exponent 2^e modulo 2^{e+2}.

Proof of Theorem 3: First assume that the integer m has property $P(n)$. We shall show that

$$m|2^{e+2}p_1^{e_1}p_2^{e_2}\dots\ p_t^{e_t}$$

by showing that:

(i) 2^{e+3} does not divide m,

(ii) for $i = 1, 2, \dots, t$, $p_i^{e_i+1}$ does not divide m, and

(iii) the only odd primes that may possibly divide m are $p_1, p_2, \dots, p_t$.

If $2^{e+3}|m$, then by Lemma 4, $5^n \equiv 1 \pmod{2^{e+3}}$. But since 5 belongs to the exponent 2^{e+1} modulo 2^{e+3}, we have the contradiction $2^{e+1}|n$.

Now suppose $p_i^{e_i+1}|m$ and let x be a primitive root modulo $p_i^{e_i+1}$. By Lemma 4, $x^n \equiv 1 \pmod{p_i^{e_i+1}}$. But this is impossible since $\phi(p_i^{e_i+1})$ does not divide n.

Similarly, suppose there is an odd prime p such that $p|m$ and $p \neq p_i$ for $i = 1, 2, \ldots, t$, and let x be a primitive root modulo p. By Lemma 4, $x^n \equiv 1 \pmod{p}$. But this is impossible since $\phi(p)$ does not divide n.

Conversely, assume

$$m | 2^{e+2}p_1^{e_1}p_2^{e_2}\ldots\, p_t^{e_t}.$$

Thus, by Lemma 4, it is sufficient to prove that $2^{e+2}p_1^{e_1}p_2^{e_2}\ldots\, p_t^{e_t}$ has property $P(n)$. So assume

$$(a,\ 2^{e+2}p_1^{e_1}p_2^{e_2}\ldots\, p_t^{e_t}) = 1.$$

Thus $(a, 2) = 1$, so by Lemma 5, $a^{2^e} \equiv 1 \pmod{2^{e+2}}$. Also, for $i = 1, 2, \ldots, t$, $(a, p_i^{e_i}) = 1$, so by the Euler-Fermat theorem,

$$a^{\phi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}.$$

Since $2^e|n$ and $\phi(p_i^{e_i})|n$ for $i = 1, 2, \ldots, t$, $a^n \equiv 1 \pmod{2^{e+2}}$ and $a^n \equiv 1 \pmod{p_i^{e_i}}$ for $i = 1, 2, \ldots, t$. Therefore,

$$a^n \equiv 1 \pmod{2^{e+2}p_1^{e_1}p_2^{e_2}\ldots\, p_t^{e_t}}.$$

2. SOME CONSEQUENCES OF $P(n)$

We shall now consider some consequences of an integer m having property $P(n)$ or a similar property. Our first result shows that an integer m having property $P(n)$ puts a restriction not just on the n^{th} powers of the integers relatively prime to m but on the n^{th} powers of all integers.

Theorem 6

Let m and n be integers with $n > 2$. The following four conditions are equivalent:

I. m has property $P(n)$.

II. For all integers a, b, k, where k is positive,

$$a^{kn} + b^{kn} \equiv a^{kn}b^{kn} + (a, b)^{kn} \pmod{m}.$$

III. For all integers a,

$$a^n \equiv (a, m)^n \pmod{m}.$$

IV. For all integers a and b, if $(ab, m) = (b, m)$, then, for all positive integers k,

$$a^{kn}b \equiv b \pmod{m}.$$

Theorem 6 is not true for $n = 2$; for $n = 2$, $m = 24$, $k = 1$, $a = 10$, and $b = 14$. I is true but II is false.

For Theorem 6, we clearly have that III implies I. Also, by letting $b = m$ and $k = 1$ in II, we see that II implies III and, by letting $b = 1$ and $k = 1$ in IV, we see that IV implies I. We shall complete the proof of Theorem 6 by showing that I implies II and that I implies IV. To show that I implies II, we shall need the following lemma, which, for the case $ab \equiv 0 \pmod{m}$ and $k = 1$, was proved in Theorem 13 of [1].

Lemma

Let n be a positive integer. If m has property $P(n)$ and $(a, b) = 1$, then, for all positive integers k,

$$a^{kn} + b^{kn} \equiv a^{kn}b^{kn} + 1 \pmod{m}.$$

Proof: Choose d and e such that

$$de = m,\ (d, e) = 1,\ (a, d) = 1, \text{ and } (b, e) = 1.$$

We can do this as follows: If $(b, m) = 1$, let $d = 1$ and $e = m$. Otherwise, let $p_1, p_2, \ldots, p_t$ be the distinct primes that divide both b and m and, for $i = 1, 2, \ldots, t$, choose $e_1, e_2, \ldots, e_t$ such that $p_i^{e_i} \| m$. Just let

$$d = p_1^{e_1}p_2^{e_2}\ldots p_t^{e_t} \quad \text{and} \quad e = \frac{m}{d}.$$

Since $d|m$, d has property $P(n)$. Thus, $a^{kn} \equiv 1 \pmod{d}$. Similarly $b^{kn} \equiv 1 \pmod{e}$. Therefore,

$$0 \equiv (a^{kn} - 1)(b^{kn} - 1) \equiv a^{kn}b^{kn} - a^{kn} - b^{kn} + 1 \pmod{m}.$$

That is,

$$a^{kn} + b^{kn} \equiv a^{kn}b^{kn} + 1 \pmod{m}.$$

Proof that I Implies II

Assume that m has property $P(n)$ and let a, b, k be integers with k positive. Let $p_1, p_2, \ldots, p_t$ be the distinct primes that divide all three of a, b, m and, for $i = 1, 2, \ldots, t$, choose e_i such that $p_i^{e_i} \| m$. Thus, there is an integer c such that

$$m = p_1^{e_1}p_2^{e_2}\ldots p_t^{e_t}c,\ (a, b, c) = 1, \text{ and } \left(c, \frac{m}{c}\right) = 1.$$

In addition, since m has property $P(n)$ and $n > 2$, $e_i \leqslant n$ for $i = 1, 2, \ldots, t$. We shall prove that I implies II by showing that

$$a^{kn} + b^{kn} \quad \text{and} \quad a^{kn}b^{kn} + (a, b)^{kn}$$

are congruent modulo c and modulo m/c.

Since c has property $P(n)$, the preceding lemma implies that

$$\frac{a^{kn}}{(a, b)^{kn}} + \frac{b^{kn}}{(a, b)^{kn}} \equiv \frac{a^{kn}b^{kn}}{(a, b)^{2kn}} + 1 \pmod{c}$$

and $((a, b), c) = 1$ implies that

$$(a, b)^{kn} \equiv 1 \pmod{c}.$$

These two congruences imply that

$$a^{kn} + b^{kn} \equiv a^{kn}b^{kn} + (a, b)^{kn} \pmod{c}.$$

Since, for $i = 1, 2, \ldots, t$, $p_i | (a, b)$ and $e_i \leqslant n \leqslant kn$, $(a, b)^{kn} \equiv 0 \pmod{m/c}$. Hence, a^{kn}, b^{kn}, and $a^{kn}b^{kn}$ are also congruent to 0 modulo m/c. Thus,

$$a^{kn} + b^{kn} \equiv 0 \equiv a^{kn}b^{kn} + (a, b)^{kn} \pmod{m/c}.$$

Proof that I Implies IV

Assume that m has property $P(n)$ and that $(ab, m) = (b, m)$. Since

$$(b,\ m) = (ab,\ m) = (ab,\ m(a,\ 1)) = (ab,\ am,\ m)$$
$$= (a(b,\ m),\ m) = (b,\ m)\left(a,\ \frac{m}{(b,\ m)}\right),$$

we have that $1 = \left(a,\ \frac{m}{(b,\ m)}\right)$. Thus,

$$a^{kn} \equiv 1 \pmod{\frac{m}{(b,\ m)}},$$

so

$$a^{kn}b \equiv b \pmod{\frac{mb}{(b,\ m)}}.$$

Therefore, $a^{kn}b \equiv b \pmod{m}$.

The equivalence, for $k = 1$, of I and III in Proposition 7, below, implies Corollary 3.1 of [5].

Proposition 7

Let m, n, r be integers where n and r are positive and m has property $P(n)$. The following three conditions are equivalent:

I. m is $(r + 1)$ power-free.

II. For all integers a, $(a^r,\ m) = (a^{r+1},\ m)$.

III. For all integers a and all positive integers k, $a^{kn+r} \equiv a^r \pmod{m}$.

Proof: It is easy to show that I and II are equivalent. Now, II implying III follows from the equivalence of Theorem 6(I) and Theorem 6(IV) with $b = a^r$. To prove that III implies II, assume that $a^{n+r} \equiv a^r \pmod{m}$. Therefore,

$$(a^r,\ m) = (a^{n+r},\ m) \geqslant (a^{r+1},\ m) \geqslant (a^r,\ m).$$

Proposition 8

Let k, m, n be integers such that k and n are positive, m has property $P(n)$, and m is $(k,\ n) + 1$ power-free. For every integer a, if the congruence

$$x^{(k,\,n)} \equiv a \pmod{m}$$

has a solution, then congruence $x^k \equiv a \pmod{m}$ has a solution.

Proof: Let a be an integer and assume that the congruence

$$x^{(k,\,n)} \equiv a \pmod{m}$$

has a solution, say $x = b$. There are positive integers u and w such that

$$ku = nw + (k,\ n).$$

Thus, by Proposition 7,

$$b^{ku} = b^{nw+(k,\,n)} \equiv b^{(k,\,n)} \equiv a \pmod{m}.$$

Therefore, the congruence $x^k \equiv a \pmod{m}$ has a solution, for example, $x = b^u$.

The restriction "m is $(k,\ n) + 1$ power-free" is needed in Proposition 8. In general, for a prime p, if $p^{(k,\,n)+1}$ divides m and $k > (k,\ n)$, then the congruence

$$x^{(k,\,n)} \equiv p^{(k,\,n)} \pmod{m}$$

will have a solution, but the congruence

$$x^k \equiv p^{(k,n)} \pmod{m}$$

will not have a solution. This is so because, for p a prime,

$$p^{(k,n)+1} | m, \; x^k \equiv p^{(k,n)} \pmod{m}, \text{ and } k > (k, n)$$

imply the contradiction

$$p^{(k,n)+1} \leqslant (x^k, m) = (p^{(k,n)}, m) = p^{(k,n)}.$$

Our next result is a generalization of Theorem 1 of [3].

Theorem 9

Let c, d, m, n be integers with n positive and $(cd, m) = 1$. The following two conditions are equivalent.

I. For all integers t, if $(t, m) = 1$, then

$$(t^n - c^n)(t^n - d^n) \equiv 0 \pmod{m}.$$

II. For all integers a and b, if $ab \equiv cd \pmod{m}$, then

$$a^n + b^n \equiv c^n + d^n \pmod{m}.$$

Proof: First assume I and assume $ab \equiv cd \pmod{m}$. Thus,

$$(a, m) \leqslant (ab, m) = (cd, m) = 1.$$

Hence, by I,

$$\begin{aligned} 0 &\equiv (a^n - c^n)(a^n - d^n) = a^{2n} - a^n d^n - a^n c^n + c^n d^n \\ &\equiv a^{2n} - a^n d^n - a^n c^n + a^n b^n = a^n(a^n - d^n - c^n + b^n) \pmod{m}. \end{aligned}$$

Therefore, since $(a, m) = 1$,

$$a^n + b^n \equiv c^n + d^n \pmod{m}.$$

Conversely, assume II and assume $(t, m) = 1$. Thus, there is an integer a such that $at \equiv cd \pmod{m}$. Hence, by II,

$$a^n + t^n \equiv c^n + d^n \pmod{m}.$$

Therefore,

$$\begin{aligned} 0 = 0t^n &\equiv (t^n - d^n - c^n + a^n)t^n = t^{2n} - d^n t^n - c^n t^n + a^n t^n \\ &\equiv t^{2n} - d^n t^n - c^n t^n + c^n d^n = (t^n - c^n)(t^n - d^n) \pmod{m}. \end{aligned}$$

Theorem 10

If an integer m has property $P(2k)$, where k is a positive integer, then there is an integer c such that $(t, m) = 1$ implies

$$(t^k - c^k)(t^k - 1^k) \equiv 0 \pmod{m}.$$

Proof: Assume $m = p_1^{e_1} p_2^{e_2} \ldots p_j^{e_j}$ has property $P(2k)$. We can choose c such that $c \equiv c_i \pmod{p_i^{e_i}}$ for $i = 1, 2, \ldots, j$, where $c_1, c_2, \ldots, c_j$ are chosen as follows:

For $p_i = 2$, $c_i = 1$ if k is an even integer and $c_j = 3$ if k is an odd integer. For p_i an odd prime, $c_i = 1$ if $p_i^{e_i}$ has property $P(k)$; otherwise, choose c_i such that $c_i^k \equiv -1 \pmod{p_i^{e_i}}$.

The converse of Theorem 10 is false. A counterexample is $k = 2$ and $m = 64$. We do have that $(t, 64) = 1$ implies that

$$(t^2 - 1)(t^2 - 1) \equiv 0 \pmod{64},$$

but 64 does not have property $P(4)$. The reason $(t^2 - 1)(t^2 - 1) \equiv 0 \pmod{64}$ is because t odd implies $8|(t^2 - 1)$.

The next theorem is a generalization of Theorem 2 of [3].

Theorem 11

Let k be an odd positive integer. The following two conditions are equivalent.

I. There is an integer d such that if $ab \equiv d \pmod{m}$, then

$$a^k + b^k \equiv 1 + d^k \pmod{m}.$$

II. m has property $P(2k)$.

Proof: Assume I and assume $(x, m) = 1$. Thus, there is an integer y such that $xy \equiv d \pmod{m}$. Since $xy \equiv d \pmod{m}$ and $(-1)(-d) \equiv d \pmod{m}$, by I,

$$x^k + y^k \equiv 1 + d^k \pmod{m} \tag{1}$$

and

$$-1 - d^k \equiv (-1)^k + (-d)^k \equiv 1 + d^k \pmod{m}. \tag{2}$$

If m is an odd integer, then by (2), $d^k \equiv -1 \pmod{m}$. Hence, by (1),

$$x^k \equiv -y^k \pmod{m}.$$

Therefore,

$$x^{2k} \equiv -x^k y^k \equiv -d^k \equiv 1 \pmod{m}.$$

If m is an even integer, then since $(x, m) = 1$ and by (2), 2 divides $x^k - 1$ and $m/2$ divides $d^k + 1$. Thus,

$$0 \equiv (d^k + 1)(x^k - 1) = d^k x^k - d^k + x^k - 1 \pmod{m}. \tag{3}$$

Therefore, by (1) and (3),

$$\begin{aligned} x^{2k} &\equiv x^k(1 + d^k - y^k) = x^k + d^k x^k - x^k y^k \\ &\equiv x^k + d^k x^k - d^k \equiv 1 \pmod{m}. \end{aligned}$$

Now assume m has property $P(2k)$. To prove I, we will prove that if $ab \equiv -1 \pmod{m}$, then $a^k + b^k \equiv 0 \pmod{m}$. Therefore, assume $ab \equiv -1 \pmod{m}$. Hence, $(a, m) = 1$. Thus,

$$0 \equiv a^{2k} - 1 \equiv a^{2k} + (ab)^k = a^k(a^k + b^k) \pmod{m}.$$

Since $(a, m) = 1$, this implies that $a^k + b^k \equiv 0 \pmod{m}$.

REFERENCES

1. John H. E. Cohn. "On m-tic Residues Modulo n." *The Fibonacci Quarterly* 5 (1967):305-18.
2. Hansraj Gupta. *Selected Topics in Number Theory*. Kent, United Kingdom: Abacus House, 1980.
3. V. C. Harris & M. V. Subbarao. "Congruence Properties of $\sigma_r(N)$." *Pacific J. Math.* 12 (1962):925-28.

4. William Judson LeVeque. *Topics in Number Theory*. Vol. I. Reading, Mass.: Addison-Wesley, 1965.
5. A. E. Livingston & M. L. Livingston. "The Congruence $a^{r+s} \equiv a^r \pmod{m}$." *Amer. Math. Monthly* 85 (1978):97-100.
6. Trygve Nagell. *Introduction to Number Theory*. Chelsea, New York, 1964.
7. C. L. Vanden Eynden. "A Congruence Property of the Divisors of n for Every n." *Duke Math. J.* 29 (1962):199-202.

◆◇◆◇◆

LETTER TO THE EDITOR

Dear Dr. Bergum:

A paper by Charles R. Wall entitled "Unitary Harmonic Numbers" appeared in the February 1983 issue of *The Fibonacci Quarterly*. We thought you might be interested in knowing that a paper with the same title and similar content was published by us (P. Hagis & G. Lord) in the *Proceedings of The American Mathematical Society*, v. 51, 1975, pp. 1-7. Comparing Wall's results with ours, you will see that both of Wall's theorems contain minor errors. Thus, there are 45 (not 43) unitary harmonic numbers less than 10^6, including $1512 = 2^3 3^3 7$ and 791700, both of which were missed by Wall. And, since $\omega(1512) = 3$, there are 24 (not 23) unitary harmonic numbers n for which $\omega(n) \leqslant 4$.

It should also be mentioned that Wall's conjecture that "there are only finitely many unitary harmonic numbers with $\omega(n)$ fixed" is Theorem 2 in our paper.

Sincerely,

Peter Hagis, Jr.

Graham Lord

RESPONSE

Dear Dr. Bergum:

Professors Hagis and Lord are correct in their observations. The omission of 1512 and 791700 resulted from an oversight which is entirely my responsibility. The duplication of their earlier work was unfortunate but done in innocence; it is doubly unfortunate that neither the referee nor I was aware of the earlier paper.

Independent but duplicate results are inevitable. One hopes that a reinvented wheel is in some way superior; in this case, alas, the earlier model was better in all respects. I apologize to you and to readers of *The Fibonacci Quarterly*.

Sincerely,

Charles R. Wall

◆◇◆◇◆