THE CONGRUENCE $x^n \equiv a \pmod{m}$, WHERE $(n, \phi(m)) = 1$

M. J. DeLEON
Florida Atlantic University, Boca Raton, FL 33431
(Submitted January 1980)

Craig M. Cordes [2] and Charles Small [4] proved Theorem 1, a result that W. Sierpinski [3] proved, using elementary group theoretic considerations, for n being a prime, and J. H. E. Cohn [1, Theorem 7] proved for $n = m$. Moreover, Theorem 1 is implicit in some of the solutions to Problem E2446 in the *American Mathematics Monthly* (January 1975).

Throughout this paper, m and n will denote positive integers with $m > 1$.

Theorem 1: Let n be greater than 1. The congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a if and only if $(n, \phi(m)) = 1$ and m is a product of distinct primes.

Let $a_1, a_2, \ldots, a_m$ be a complete residue system modulo m. It follows from Theorem 1 that $a_1^n, a_2^n, \ldots, a_m^n$, where $n > 1$, is a complete residue system modulo m if and only if $(n, \phi(m)) = 1$ and m is a product of distinct primes.

We shall give a simple proof of Theorem 1 and, in addition, prove the following two related results.

Theorem 2: The following three conditions are equivalent.

I. The congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a with
$$\left(a, \frac{m}{(a, m)}\right) = 1.$$

II. The congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a relatively prime to m.

III. $(n, \phi(m)) = 1$.

From Theorem 2, it follows that for $a_1, a_2, \ldots, a_{\phi(m)}$ a reduced residue system modulo m, $a_1^n, a_2^n, \ldots, a_{\phi(m)}^n$ is a reduced residue system modulo m if and only if $(n, \phi(m)) = 1$.

The following result tightens the equivalence of Theorem 2.

Theorem 3: Conditions I and II are equivalent.

I. The congruence $x^n \equiv a \pmod{m}$ has a solution if and only if
$$\left(a, \frac{m}{(a, m)}\right) = 1.$$

II. $(n, \phi(m)) = 1$ and $p^{n+1} \nmid m$ for all primes p.

By Theorem 3, we can, with only the simplest of calculations, write down the nth-power residues modulo m if $(n, \phi(m)) = 1$ and $p^{n+1} \nmid m$ for all primes p.

We shall now state and prove several results needed for the proofs of these three theorems.

Lemma 4: Let a and n be positive integers. If $\left(\;, \frac{m}{(a, m)}\right) = 1$, then there is a positive integer t such that

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

Proof: Assume $\left(a, \frac{m}{(a, m)}\right) = 1$ and, for convenience, let $d = (a, m)$. Since

$$\left(a, \frac{m}{d}\right) = 1 \quad \text{and} \quad \phi\left(\frac{m}{d}\right) \mid \phi(m),$$

by the Euler-Fermat theorem,

$$a^{\phi(m)} \equiv 1 \left(\operatorname{mod} \frac{m}{d}\right).$$

There are positive integers c and t such that $nt - (n, \phi(m)) = \phi(m)c$. Thus

$$a^{nt-(n, \phi(m))} \equiv a^{\phi(m)c} \equiv 1 \left(\operatorname{mod} \frac{m}{d}\right).$$

Hence

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

Corollary 5: If $(n, \phi(m)) = 1$, then the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a with $\left(a, \frac{m}{(a, m)}\right) = 1$.

Corollary 6: If $(n, \phi(m)) = 1$ and m is a product of distinct primes, then the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a.

Corollary 6 follows directly from Lemma 4 since m being a product of distinct primes implies $\left(a, \frac{m}{(a, m)}\right) = 1$ for every integer a.

Lemma 7: If the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a relatively prime to m, then $(n, \phi(m)) = 1$.

Proof: Assume $(n, \phi(m)) \neq 1$. Thus, there is a prime q such that $q \mid n$ and $q \mid \phi(p^e)$, where $p^e \| m$ and p is a prime. We shall show that the assumption $p = 2$ leads to a contradiction and that the assumption $p > 2$ also leads to a contradiction.

First, assume $p = 2$. Thus, q divides $\phi(2^e) = 2^{e-1}$ so $q = 2$ and $e \geq 2$. Choose a such that $a \equiv 3 \pmod{2^e}$ and $a \equiv 1 \pmod{m/2^e}$. Thus $(a, m) = 1$; so, by assumption, the congruence $x^n \equiv a \pmod{m}$ has a solution. Since $4 \mid 2^e$ and $2^e \mid m$, we have $4 \mid m$. Hence, the congruence $x^n \equiv a \equiv 3 \pmod{4}$ has a solution. But $x^n \equiv 3 \pmod{4}$ is impossible, since n is divisible by $q = 2$.

Now assume $p > 2$. Choose a such that a is a primitive root modulo p^e and $a \equiv 1 \pmod{m/p^e}$. Thus $(a, m) = 1$, so there is an integer x such that $x^n \equiv a \pmod{m}$. Since $p^e \mid m$, $x^n \equiv a \pmod{p^e}$. For $k = \phi(p^e)/q$, $a^k \equiv x^{nk} \equiv 1 \pmod{p^e}$.

The last congruence is true because $\phi(p^e) = qk$, which divides nk. But $a^k \equiv 1 \pmod{p^e}$ is impossible, since a is a primitive root modulo p^e and

$$0 < k < \phi(p^e).$$

We shall now prove Theorem 1. First, assume that the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a. Thus $0, 1, 2, \ldots, (m - 1)$ must be incongruent modulo m. Now if there is a prime p such that $p^2|m$ then, since $n > 1$, we would have the contradiction

$$0^n \equiv 0 \equiv \left(\frac{m}{p}\right)^n \pmod{m}.$$

Therefore, m must be a product of distinct primes. By Lemma 7, we have that $(n, \phi(m)) = 1$.

Conversely, assume $(n, \phi(m)) = 1$ and m is a product of distinct primes. By Corollary 6, the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a.

We shall now prove Theorem 2. Since $(a, m) = 1$ implies $\left(a, \dfrac{m}{(a, m)}\right) = 1$, II follows from I. The remaining implications—II implies III and III implies I—follow from Lemma 7 and Corollary 5, respectively.

To prove Theorem 3, we need

Lemma 8: Let a be an integer. If $p^{n+1} \nmid m$ for all primes p and the congruence $x^n \equiv a \pmod{m}$ has a solution, then $\left(a, \dfrac{m}{(a, m)}\right) = 1$.

Proof: Assume the congruence $x^n \equiv a \pmod{m}$ has a solution and there is a prime p such that $p|a$ and $p\left|\dfrac{m}{(a, m)}\right.$. Choose e such that $p^e \| m$; clearly $e \leq n$. Since $p|a$ and $p|m$, $p|x^n$; so $p^e|x^n$. From $p^e|m$ and $p^e|x^n$, we have that $p^e|a$, so $p^e|(a, m)$. But since $p\left|\dfrac{m}{(a, m)}\right.$, too, we have the contradiction $p^{e+1}|m$.

Finally, we prove Theorem 3. First, assume condition I. Thus, in particular, the congruence $x^n \equiv a \pmod{m}$ has a solution for every integer a relatively prime to m. Hence, by Lemma 7, $(n, \phi(m)) = 1$. To prove that $p^{n+1} \nmid m$ for all primes p, assume there is a prime p such that $p^{n+1}|m$. Thus

$$\left(p^n, \frac{m}{(p^n, m)}\right) = \left(p^n, \frac{m}{p^n}\right) \geq p > 1.$$

Therefore, by condition I, the congruence $x^n \equiv p^n \pmod{m}$ has no solution. But clearly $x = p$ is a solution to the congruence $x^n \equiv p^n \pmod{m}$.

The fact that condition II implies condition I follows from Lemma 8 and Corollary 5.

References

1. John H. E. Cohn. "On m-tic Residues Modulo n." *The Fibonacci Quarterly* 5, no. 4 (1967):305-318.

2. Craig M. Cordes. "Permutations Mod m in the Form x^n." *Amer. Math. Monthly* 83 (1976):32-33.
3. W. Sierpinski. "Contribution a l'étude des restes cubiques." *Ann. Soc. Polon. Math.* 22 (1949):269-272 (1950).
4. Charles Small. "Powers Mod n." *Math. Mag.* 50 (1977):84-86.

*****

ON THE ENUMERATION OF CERTAIN COMPOSITIONS AND RELATED SEQUENCES OF NUMBERS

CH. A. CHARALAMBIDES
University of Athens, Panepistemiopolis, Athens 621, Greece
(Submitted February 1981)

Abstract

The numbers

$$A(m,\ k,\ s,\ r) = [\nabla^{m+1}\mathrm{E}^k\underline{(sx+r)_m}]_{x=0},$$

where $\nabla = 1 - \mathrm{E}^{-1}$, $\mathrm{E}^j f(x) = f(x+j)$, $\underline{u}_x = u_x$ when $0 \leq x \leq k$ and $\underline{u}_x = 0$ otherwise, $(y)_m = y(y-1)\ \ldots\ (y-m+1)$, are the subject of this paper. Recurrence relations, generating functions, and certain other properties of these numbers are obtained. They have many similarities with the Eulerian numbers

$$A_{m,k} = \frac{1}{m!}[\nabla^{m+1}\mathrm{E}^k\underline{x^m}]_{x=0},$$

and give in particular (i) the number $C_{m,n,s}$ of compositions of n with exactly m parts, no one of which is greater than s, (ii) the number $Q_{s,m}(k)$ of sets $\{i_1,\ i_2,\ \ldots,\ i_m\}$ with $i_n \in \{1,\ 2,\ \ldots,\ s\}$ (repetitions allowed) and showing exactly k increases between adjacent elements, and (iii) the number $Q_{s,m}(r,\ k)$ of those sets which have $i_1 = r$. Also, they are related to the numbers

$$G(m,\ n,\ s,\ r) = \frac{1}{n!}[\Delta^n(sx+r)_m]_{x=0},\quad \Delta = \mathrm{E} - 1,$$

used by Gould and Hopper [11] as coefficients in a generalization of the Hermite polynomials, and to the Euler numbers and the tangent-coefficients T_m. Moreover, $\lim\limits_{s\to\pm\infty} s^{-m}m!A(m,\ k,\ s,\ su) = A_{m,k,u}$, where

$$A_{m,k,u} = \frac{1}{m!}[\nabla^{m+1}\mathrm{E}^k\underline{(x+u)^m}]_{x=0}$$

is the Dwyer [8, 9] cumulative numbers; in particular,

$$\lim_{s\to\pm\infty} s^{-m}m!A(m,\ k,\ s) = A_{m,k},\quad A(m,\ k,\ s) \equiv A(m,\ k,\ s,\ 0).$$

Finally, some applications in statistics are briefly discussed.