RESIDUES — PART III
CONGRUENCES TO GENERAL COMPOSITE MODULI

Joseph B. Dence and Thomas P. Dence

1. Introduction. Every introductory text on number theory presents Euler's Criterion: a positive integer A is a quadratic residue of the odd prime p if and only if

$$A^{(p-1)/2} \equiv 1 \pmod{p}.$$

But what criterion could one use for arbitrary power residues of arbitrary moduli, even those that do not possess primitive roots [1]? This is generally not discussed, and so in this paper we address this question in a manner that is suitable for classroom presentation. Our final result is Theorem 6, which may be regarded as a generalization of Euler's Criterion and is a continuation of our earlier work on residues [2], [3].

2. Some Preliminary Results for Composite Moduli. We quote in this section two well–known results (Theorems 1 and 3) that we shall need. The first result is for moduli that are powers of a single odd prime. The proof is standard [2], [4] and makes use of the fact that a power of an odd prime has a primitive root.

<u>Theorem 1</u>. Let $p > 2$ be a prime and let n, k be positive integers. Then A is a kth–power residue of p^n if and only if $A^{\phi(p^n)/d} \equiv 1 \pmod{p^n}$, where ϕ is the Euler phi–function and $d = (k, \phi(p^n))$.

Easily constructed counterexamples show that the theorem is false for $p = 2$. Nevertheless, for odd p the theorem provides a systematic, albeit tedious, way of ascertaining the kth–power residues of p^n.

By Euler's Theorem it is only necessary to consider the case $k \leq \phi(p^n)$. Then, although it is not our focus here to detail the explicit calculation of the kth–power residues of p^n, it is possible to prove the following theorem, which by repeated application can in many cases relieve some of the tedium of Theorem 1.

<u>Theorem 2</u>. Let $p > 2$ be prime and let m, n, k be positive integers that satisfy $1 < k \leq \phi(p^m) < \phi(p^n)$. Let $\{A_i\}$ be the least–positive kth–power residues of p^m. Then the least–positive kth–power residues of p^{m+1} are the numbers $\{A_i + ap^m : a = 0, 1, 2, \cdots, p-1\}$.

For example, by trial (or by Theorem 1) we find that 7 is a quartic residue of 9. Suppose we desire some quartic residues of 81. Then Theorem 2 shows that 7, 16, 25 are quartic residues of 27, and one more application of Theorem 2 yields 7, 34, 61; 16, 43, 70; 25, 52, 79 as *some* of the quartic residues of 81.

The second standard result looks at polynomial congruences with an arbitrary modulus m, where m is written in canonical form as

$$m = \prod_{i=1}^{r} p_i^{\alpha_i},$$

and each p_i is a distinct prime [5].

Theorem 3. Let $f(x) \in \mathbb{Z}[x]$ and let m be represented as above. Then the congruence

$$f(x) \equiv 0 \pmod{m}$$

has a solution x if and only if

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$$

has a solution for each i.

The theorem is an immediate consequence of the Chinese Remainder Theorem, and automatically includes the case where m contains powers of 2 in its canonical decomposition.

3. Moduli That Are Powers of Two. Table 1 shows that there is systematic behavior among the residues A in $x^k \equiv A \pmod{2^n}$ when k is even. This contrasts sharply with the case when k is odd; there, the residues A are not limited to particular odd integers [3].

Table 1. Least–Positive Even–Power Residues of 2^n

k	$n=4$	$n=6$	$n=7$
$2\cdot 3\cdot 5$	1,9	1,9,17,25,33,41,49,57	$1,9,17,25,\cdots,121$
$2^2\cdot 5^2$	1	1,17,33,49	1,17,33,49,65,81,97,113
$2^2\cdot 3$	1	1, 33	1,33,65,97
2^3	1	1,33	1,33,65,97

Of course, when $k=2^{n-1}$ there is only one least–positive kth–power residue. Less well–known is the fact that this is also true when $k=2^{n-2}$, $n\geq 3$. It certainly holds when the modulus is $8(n=3)$; assume it also holds for the modulus 2^n. Then for *any* odd x

$$x^{2^{n-2}}\equiv 1 \pmod{2^n},$$

or $x^{2^{n-2}}=1+b\cdot 2^n$ for some positive integer b. If x_0 is a presumed solution to $x^{2^{n-1}}\equiv A \pmod{2^{n+1}}$, then

$$\begin{aligned} x_0^{2^{n-1}} &= (x_0^{2^{n-2}})^2=(1+b\cdot 2^n)^2=1+b\cdot 2^{n+1}+b^2\cdot 2^{2n} \\ &\equiv 1 \pmod{2^{n+1}} \\ &\equiv A \pmod{2^{n+1}}. \end{aligned}$$

Hence, by induction we obtain the following theorem.

Theorem 4. If $k=2^{n-2}$ and $n\geq 3$, then 1 is the only least–positive kth–power residue of 2^n.

Corollary 4.1. If $k=2^d$, $d\leq n-2$. Then the least–positive kth–power residues of 2^n are the numbers $\{1+2^{d+2}\sigma:\sigma=0,1,\cdots,2^{n-d-2}-1\}$.

Proof. By Theorem 4 there is one (2^dth)–power residue of 2^{d+2}. Theorem 2 can be extended to cover the case $p=2$; then there are just two (2^dth)–power residues of 2^{d+3}, and these differ by 2^{d+2}. This difference is maintained among the (2^dth)–power residues of 2^{d+4}, among the (2^dth)–power residues of 2^{d+5}, and so on. For the modulus $m=2^n$ we observe that $1+(2^{d+2})(2^{n-d-2})=1+m$, so the least–positive (2^dth)–power residues of 2^n are the numbers of the form $1+2^{d+2}\sigma$, where the integer σ runs from 0 to $2^{n-d-2}-1$.

The Corollary generalizes theorems from [3]: A is a quadratic residue modulo 2^n if and only if $A = 8k+1$, and A is a quartic residue modulo 2^n if and only if $A = 16k+1$. In general, if $n \geq d+2$, then there are 2^{n-d-2} (2^dth)–power residues of 2^n.

Corollary 4.2. Let A be a (2^dth)–power residue of 2^n, $n \geq d+2$. Then A has exactly 2^{d+1} incongruent 2^d–th roots modulo 2^n.

Proof. Let $G = \{g_1 = 1, g_2, \cdots, g_v\}$ be the group of order $v = \phi(2^n)$ of positive integers less than and relatively prime to 2^n; let $H = \{h_1, h_2, \cdots, h_r\}$ be the set of least–positive 2^d–th roots of unity modulo 2^n. Then H is a subgroup of G, and we can construct the set of *distinct* cosets of $H : \{g_1 H = H, g_2 H, \cdots, g_s H\}$. Each member of a given coset is a 2^d–th root of a fixed (2^d–th)–power residue. Elements from two different cosets cannot be 2^d–th roots of the same residue, for if $g_i H, g_j H$ had such elements, then $g_i^{2^d} \equiv g_j^{2^d} \pmod{2^n}$ would hold. Both g_i, g_j possess inverses, so we obtain for some $h_k \in H$

$$(g_i g_j^{-1})^{2^d} \equiv h_k^{2^d} \equiv 1 \pmod{2^n},$$

and therefore $g_i = g_j h_k$. This says that g_i belongs to the coset $g_j H$, a contradiction.

All of the cosets of H are the same size [6]. It follows that the 2^d–th roots of the various (2^dth)–power residues are equinumerous, namely, r, where

$$\begin{aligned} r &= \frac{\text{no. integers coprime to } 2^n}{\text{no. cosets}} = \frac{\phi(2^n)}{s} \\ &= \frac{\text{no. integers coprime to } 2^n}{\text{no. residues}} \\ &= \frac{\phi(2^n)}{2^{n-d-2}} \\ &= 2^{d+1}. \end{aligned}$$

The third equality above follows from Corollary 4.1.

Thus, 1 has four square roots ($d = 1$), eight fourth roots ($d = 2$), and so on, modulo 2^n, when $n \geq d+2$. The fourth roots of 1 modulo 128 are found to be 1, 31, 33, 63, 65, 95, 97, and 127 [7]. In contrast, when the modulus is an odd prime, there are always only 2 or 4 incongruent fourth roots of unity [2]. Their distribution is not well understood [8].

The data of Table 1 suggest that when $k = 2^d m$, $m =$ odd, then the kth–power residues of 2^n follow the same pattern as do the (2^dth)–power residues.

<u>Theorem 5</u>. Let $k = 2^d c, c \geq 3$ odd, and let n be a positive integer. Then the kth–power residues of 2^n are the (2^dth)–power residues of 2^n.

<u>Proof</u>. The least–positive $(2^d c\text{–th})$–power residues of 2^n are the intersection of the set S_1 of least–positive cth–power residues of 2^n and the set S_2 of least–positive (2^dth)–power residues of 2^n. But S_1 is all the odd integers in $[1, 2^n - 1]$ [3], and S_2 is given by Corollary 4.1 if $n \geq d+2$, or by the singleton set $\{1\}$ if $n < d+2$. Hence, $S_1 \cap S_2 = S_2$, and this is the theorem.

4. General Moduli. The results of the previous sections can finally be assembled to give us the main theorem for arbitrary moduli m, now represented by

$$m = 2^n \prod_{i=1}^{r} p_i^{\alpha_i},$$

where the p_i's are odd primes.

<u>Theorem 6</u>. (Generalized Euler Criterion.) Let $k = 2^d c > 1, (2, c) = 1$ and let the modulus m be defined as above. Then A is a kth–power residue of m if and only if

$$A^{\phi(p_i^{\alpha_i})/d_i} \equiv 1 \pmod{p_i^{\alpha_i}},\ d_i = (k, \phi(p_i^{\alpha_i}))$$

for $i = 1, 2, \cdots, r$, and if and only if

$$A \equiv \begin{cases} 1 + 2^{d+2}\sigma \pmod{2^n}, \sigma \in [0, 2^{n-d-2} - 1] & \text{if } n \geq d+2 > 2 \\ 1 \pmod{2^n} & \text{if } 0 < n < d+2. \end{cases}$$

<u>Proof</u>. Let $f(x) = x^k - A$. By Theorem 3 we have $f(x) \equiv 0 \pmod m$ is solvable if and only if for $i = 1, 2, \cdots, r$,

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$$

is solvable and if and only if $f(x) \equiv 0 \pmod{2^n}$ is solvable. The congruences involving the p_i's hold if and only if

$$A^{\phi(p_i^{\alpha_i})/d_i} \equiv 1 \pmod{p_i^{\alpha_i}}$$
$$d_i = (k, \phi(p_i^{\alpha_i})),$$

according to Theorem 1. If $n = 0$, we are done.

If $n > 0$ but $d = 0$, the congruence

$$x^k - A \equiv 0 \pmod{2^n}$$

is solvable if and only if A is any odd integer [3]. However, when $n, d > 0$ then from Theorem 5

$$x^k - A \equiv 0 \pmod{2^n}$$

is solvable if and only if A is a (2^dth)–power residue of 2^n, that is (Corollary 4.1), if and only if A is congruent modulo 2^n to a number of the form

$$1 + 2^{d+2}\sigma, \sigma \in [0, 2^{n-d-2} - 1]$$

when $d \leq n - 2$, or is congruent modulo 2^n to 1 when $0 < n < d + 2$ (Theorem 4).

Example. $x^{40} \equiv A \pmod{1344}$. Here, $n = 6$, $d = 3$, $c = 5$, $n - d - 2 = 1$, $p_1 = 3$, $p_2 = 7$. Theorem 5 gives as criteria for A:

$$\begin{cases} A \equiv 1 \pmod{3} \\ A^3 \equiv 1 \pmod{7} \\ A \equiv 1 \text{ or } 33 \pmod{64}. \end{cases}$$

The second congruence yields $A \equiv 1, 2$ or $4 \pmod{7}$. The allowed A's can now be found from repeated applications of the Chinese Remainder Theorem. For example, the unique solution (modulo 1344) to the system

$$\begin{cases} A \equiv 1 \pmod{3} \\ A \equiv 2 \pmod{7} \\ A \equiv 33 \pmod{64}. \end{cases}$$

is $A = 289$. Indeed, by trial and error one finds $5^{40} \equiv 289 \pmod{1344}$.

References

1. H. E. Rose, *A Course in Number Theory*, Oxford University Press, Oxford, (1988), 83–84.
2. J. B. Dence and T. P. Dence, "Cubic and Quartic Residues Modulo a Prime," *Missouri Journal of Mathematical Sciences*, 7 (1995), 24–31.
3. J. B. Dence and T. P. Dence, "Residues–Part II, Congruences Modulo Powers of 2," *Missouri Journal of Mathematical Sciences*, 8 (1996), 26–35.
4. K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd ed., Addison–Wesley, Reading, (1993), 301–302.
5. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, (1976), 118–119.
6. J. B. Fraleigh, *A First Course in Abstract Algebra*, 5th ed., Addison–Wesley, Reading, (1994), 121.
7. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th ed., John Wiley, New York, (1980), 98.
8. S. M. Turner, "Square Roots mod p," *American Mathematical Monthly*, 101, (1994), 443–449.

Joseph B. Dence
Department of Chemistry
University of Missouri–St. Louis
St. Louis, MO 63121

Thomas P. Dence
Department of Mathematics
Ashland University
Ashland, OH 44805