RESIDUES – Part II

CONGRUENCES MODULO POWERS OF 2

Joseph B. Dence and Thomas P. Dence

A previous paper [1] summarized some theorems on cubic and quartic residues modulo an odd prime. These results may be regarded as extensions of corresponding theorems for quadratic residues modulo a prime. In the present paper we present, as the next logical step, some results on congruences modulo powers of the single prime 2. Certain of these results are formulas which are not well-known. They are not usually encountered in introductory number theory texts, but could form the basis for one or two lectures in a first course on number theory.

1. Quadratic Residues. A kth-power residue modulo m is an integer $A \neq 0$ such that $(A, m) = 1$ and the congruence $x^k \equiv A \pmod{m}$ is solvable [2]. The residues A in the cases of $k = 2, 3, 4$ are referred to as quadratic, cubic, and quartic residues, respectively, and if $m = 2^n$ these residues are necessarily odd. For the remainder of this article we shall assume that A is a least positive residue, that is, $1 \leq A < 2^n$.

Theorem 1. If A is a quadratic residue modulo 2^n, then $A = 8k + 1$, for some nonnegative integer k.

Proof. The theorem is trivially true for $n = 1, 2$, and for $A = 1$, so assume $n \geq 3$ and $k > 0$. Since A is odd, then any solution x_0 of $x^2 \equiv A \pmod{2^n}$ must be odd. Let $x_0 = 2j + 1$; then $x_0^2 = 4j^2 + 4j + 1 = 4j(j+1) + 1 = 8m + 1$, $m > 0$, since either j or $j + 1$ must be even. Hence, we have

$$8m + 1 \equiv A \pmod{2^n}$$

and as $n \geq 3$, then A itself is of the form $8k + 1$.

Table 1 gives all of the incongruent quadratic residues modulo 2^7, along with a solution x_0 in each case, of $x^2 \equiv A \pmod{2^7}$.

A	x_0	A	x_0
1	1	65	31
9	3	73	29
17	23	81	9
25	5	89	27
33	47	97	49
41	13	105	19
49	7	113	25
57	43	121	53

Table 1. Quadratic Residues Modulo 128

We notice that every A is of the form $8k+1$; this suggests the converse of Theorem 1.

Theorem 2. If $A = 8k+1$, $k \geq 0$, then $x^2 \equiv A \pmod{2^n}$ is solvable.

Proof. By listing the particular cases, one can show that the theorem is true for $1 \leq n \leq 5$; hence, assume that $n \geq 6$. The theorem then holds trivially for $A = 1$; assume it also holds for $A = A_0 = 8k_0 + 1$, with n fixed, and that $x = x_0$ is a solution in this case. Consider next

$$\begin{aligned}(3x_0 + B \cdot 2^{n-2})^2 &\equiv 8(k_0+1)+1 \pmod{2^n}\\ &\equiv A_0 + 8 \pmod{2^n},\end{aligned}$$

where B is to be determined. After expansion of the binomial on the left-hand side, we obtain

$$(3x_0 \cdot 2^{n-1})B \equiv 8(1-A_0) \quad \pmod{2^n},$$

upon making use of $9x_0^2 \equiv 9A_0 \pmod{2^n}$ and $B^2 \cdot 2^{2n-4} \equiv 0 \pmod{2^n}$, $n \geq 4$.

Let $z = 2^{n-6} \cdot B$, so that the above congruence becomes

$$(96x_0)z \equiv -64k_0 \quad \pmod{2^n},$$

or

$$(3x_0)z \equiv -2k_0 \quad \pmod{2^{n-5}}.$$

But as x_0 is odd and $(3x_0, 2^{n-5}) = 1$, then this congruence has a unique solution $z \equiv z_0 \pmod{2^{n-5}}$. It follows that $B \cdot 2^{n-2} = 16z_0$, and so $x \equiv 3x_0 + 16z_0 \pmod{2^n}$ is a solution to $x^2 \equiv A_0 + 8 \pmod{2^n}$. The theorem then follows from the Principle of Mathematical Induction.

Thus, from Table 1 let $A_0 = 25$, $k_0 = 3$, $x_0 = 5$. Then a solution of $15z \equiv -6 \pmod{4}$ is $z_0 \equiv 2 \pmod{4}$, and so $x \equiv 15 + 16 \cdot 2 \equiv 47 \pmod{128}$ is a solution to $x^2 \equiv 33 \pmod{128}$.

Corollary 2.1. The number of incongruent quadratic residues modulo 2^n is 1 if $n = 1$ or 2, and $\frac{1}{4}\phi(2^n) = 2^{n-3}$ if $n \geq 3$.

We may be interested to ascertain how often the congruence

$$x^2 \equiv A \pmod{2^n}$$

is solvable, where A is even and $2 \leq A < s^n$. Any such values of A that permit a solution do not qualify as quadratic residues modulo 2^n, but let us write, nevertheless,

$$x^2 \equiv 2^a r \pmod{2^n},$$

where $2 \leq 2^a r < 2^n$ and r is odd. If a is even, this reduces to $u^2 \equiv r \pmod{2^{n-a}}$, and this is solvable if and only if $r \equiv 1 \pmod{2^3}$ from Theorems 1 and 2. If a is odd, the congruence becomes $2u^2 \equiv r \pmod{2^{n-a}}$, and this is not solvable. Hence, we have

Corollary 2.2. The number of even integers A in the interval $2 \leq A < 2^n$ for which $x^2 \equiv A \pmod{2^n}$ is solvable is the number $E_2(n)$ of integers of the form $2^a r$, where $4 \leq 2^a r < 2^n$, $a > 0$ is even, and $r = 8k + 1$.

Some values of the number $E_2(n)$ in Corollary 2.2 are listed in Table 2 for the first few n.

n	$E_2(n)$	n	$E_2(n)$
2	0	7	6
3	1	8	11
4	1	9	22
5	2	10	43
6	3	11	86

Table 2. Values of the Function $E_2(n)$

Given n, the number of allowed values of r in Corollary 2.2 is 2^{n-3}. The total number T_n of products $2^a r$ satisfying the conditions of Corollary 2.2 depends on whether n is odd or even. When n is odd we find by induction that

$$T_n = 1 + \sum_{k=0}^{(n-5)/2} 4^k = \frac{2+2^{n-3}}{3} \quad (n \geq 5),$$

and when n is even the result is

$$T_n = 1 + \sum_{k=0}^{(n-6)/2} 2 \cdot 4^k = \frac{1+2^{n-3}}{3} \quad (n \geq 6).$$

These formulas are also accurate for $n = 3, 4$, respectively. Finally, combining these formulas with Corollary 2.1 gives

Corollary 2.3. The number of integers A in the interval $1 \leq A < 2^n$ for which $x^2 \equiv A \pmod{2^n}$ is solvable is $(2+2^{n-1})/3$ when $n \geq 1$ is odd, and is $(1+2^{n-1})/3$ when $n \geq 2$ is even.

The contrast with the case when the modulus is a prime is startling. Thus, $2^{12} = 4096$ has $(1+2^{11})/3 = 683$ integers A (of which, only 512 are actually quadratic residues) for which $x^2 \equiv A \pmod{2^{12}}$ is solvable, whereas the nearest prime of 4093 has 2046 such integers A (all of which are quadratic residues).

2. Cubic Residues. An odd prime p has either $p-1$ or $(p-1)/3$ incongruent cubic residues, according as $p = 3k+2$ or $p = 3k+1$ [1]. The pattern is different when the modulus is 2^n, as the next theorem shows.

Theorem 3. If $k \geq 3$ is odd, then every odd A satisfying $1 \leq A < 2^n$ is a kth-power residue modulo 2^n, for all $n \in \mathbb{Z}^+$.

Proof. Let $\{x_1, x_2, \ldots, x_{2^{n-1}}\}$ be the odd integers $\{1, 3, \ldots, 2^n - 1\}$. Corresponding to each x_i we compute A_i, the least positive kth-power residue modulo 2^n. Suppose $x_i \neq x_j$ but $A_i = A_j$, for some i, j. Then

$$x_i^k - x_j^k \equiv 0 \pmod{2^n}$$

or

$$(x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1}) \equiv 0 \pmod{2^n}.$$

The binomial factor $x_i - x_j$ is divisible by at most $n-1$ powers of 2 since $x_i, x_j < 2^n$. The polynomial factor is the sum of an odd number of odd terms and so is not divisible by 2. The contradiction implies $A_i \neq A_j$, and therefore the A_i's appear merely as a permutation of the x_i's.

In an exercise, Rosen [3] asserts that our Theorem 3 holds, even if k is not odd. This assertion is false. For example, 3 is not a quartic residue modulo 8. Furthermore, Rosen's "proof" begins by supposing 2^n to have a primitive root, which is false for $n > 2$.

Table 3 gives the least positive solution x_0 to the congruence $x^3 \equiv A \pmod{2^n}$ for $n = 5$ and for every odd A in the interval $[1, 31]$. We notice that $x_0^3 \equiv A \pmod{2^5}$ implies $A^3 \equiv x_0 \pmod{2^5}$. This interesting behavior also holds for moduli $2, 4, 8, 16$, but it is not general for moduli of the form 2^n.

A	x_0	A	x_0
1	1	17	17
3	27	19	11
5	29	21	13
7	23	23	7
9	25	25	9
11	19	27	3
13	21	29	5
15	15	31	31

Table 3. Cubic Residues Modulo 32

Theorem 4. If A is odd and $1 \leq A < 2^n$, then $x^3 \equiv A \pmod{2^n}$ implies $A^3 \equiv x \pmod{2^n}$ only for $n = 1, 2, 3, 4, 5$.

Proof. If $x^3 \equiv A \pmod{2^n}$, then $A^3 \equiv (Ax)^2 x \pmod{2^n}$, so $A^3 \equiv x \pmod{2^n}$ holds if and only if $(Ax)^2 \equiv 1 \pmod{2^n}$, or $x^8 \equiv 1 \pmod{2^n}$, for all odd x. This latter congruence holds for $n = 4$ from Euler's theorem, and hence, also for

$n = 1, 2, 3$. That it also holds for $n = 5$ follows from writing the congruence $x^8 \equiv 1 \pmod{2^5}$ equivalently as

$$(x^4 + 1)(x^2 + 1)(x + 1)(x - 1) \equiv 0 \pmod{2^5},$$

and noting that exactly one of the factors $x + 1, x - 1$ must be congruent to 0 (mod 4). However, $3^8 \not\equiv 1 \pmod{2^n}$ for all $n \geq 6$. This proves the theorem.

Now consider even A that permit solutions of $x^3 \equiv A \pmod{2^n}$. Write $A = 2^a r$, where $2 \leq 2^a r < 2^n$ and $r \geq 1$ is odd. By reasoning parallel to that used for Corollary 2.2, we deduce

Theorem 5. The number of even integers A in the interval $2 \leq A < 2^n$ for which $x^3 \equiv A \pmod{2^n}$ is solvable is the number $E_3(n)$ of integers of the form $2^a r$, where $8 \leq 2^a r < 2^n$, $3|a$, and $1 \leq r$ is odd.

For comparison with the quadratic case, we list in Table 4 the values of the function $E_3(n)$ in Theorem 5 for the first few n. For $n \geq 6$ we have $E_3(n) > E_2(n)$.

n	$E_3(n)$	n	$E_3(n)$
2	0	7	9
3	0	8	18
4	1	9	36
5	2	10	73
6	4	11	146

Table 4. Values of the Function $E_3(n)$

As with the quadratic case, the total number T_n of products $2^a r$ satisfying the conditions of Theorem 5 depends on the form of n. When $n = 3k$ we find by induction that

$$T_n = \sum_{m=0}^{k-2} 4 \cdot 8^m = \frac{2^{n-1} - 4}{7} \quad (n \geq 3),$$

when $n = 3k - 1$, then

$$T_n = \sum_{m=0}^{k-2} 2 \cdot 8^m = \frac{2^{n-1} - 2}{7} \quad (n \geq 2),$$

and when $n = 3k - 2$, then

$$T_n = \sum_{m=0}^{k-2} 8^m = \frac{2^{n-1} - 1}{7} \quad (n \geq 4).$$

Combination of these formulas with Theorem 3 yields, analogous to Corollary 2.3,

Corollary 5.1. The number of integers A in the interval $1 \leq A < 2^n$ for which $x^3 \equiv A \pmod{2^n}$ is solvable is

$$\begin{cases} 1, & \text{if } n = 1; \\ (2^{n+2} - 4)/7, & \text{if } n = 3k; \\ (2^{n+2} - 2)/7, & \text{if } n = 3k - 1; \\ (2^{n+2} - 1)/7, & \text{if } n = 3k - 2. \end{cases}$$

Simple comparison shows that for all $n > 1$ the number of integers A in the interval $1 \leq A < 2^n$ for which $x^3 \equiv A \pmod{2^n}$ is solvable exceeds the number for which $x^2 \equiv A \pmod{2^n}$ is solvable. This is possibly counter to intuition.

4. Quartic Residues. A result analogous to Theorems 1 and 2 holds for quartic residues and may be established by similar means.

Theorem 6. The integer A is a quartic residue modulo 2^n if and only if $A = 16k + 1$ for k a nonnegative integer.

Proof. ($\Rightarrow$) Suppose A_0 is a quartic residue modulo 2^n and let $x_0 = 2j + 1$ be a solution of $x^4 \equiv A_0 \pmod{2^n}$. Then

$$x_0^4 = 16j^4 + 32j^3 + 24j^2 + 8j + 1 = 8j(j+1)(2j^2 + 2j + 1) + 1 = 16m + 1, \ m > 0$$

(the case $m = 0$ is trivial). Hence, we have

$$16m + 1 \equiv A_0 \pmod{2^n}$$

and as we may assume $n \geq 4$ (because the lower cases can be disposed of directly), then A_0 itself is of the form $16k + 1$.

($\Leftarrow$) The theorem can be shown directly to hold in this direction for $n \leq 7$. Hence, assume $n \geq 8$ and that the theorem holds for $A = A_0 = 16k_0 + 1$; let x_0 be a solution in this case. We now consider

$$x^4 \equiv A_0 + 16 \pmod{2^n}$$

and set $x = 3x_0 + B \cdot 2^{n-3}$, where B is to be determined. Substitution and simplification yield

$$(27x_0^3)z \equiv -1 - 20k_0 \pmod{2^{n-6}},$$

where $z = B \cdot 2^{n-7}$. The congruence has a unique solution $z \equiv z_0 \pmod{2^{n-6}}$ since $(27x_0^3, 2^{n-6}) = 1$. It follows that

$$x = 3x_0 + 2^4(B \cdot 2^{n-7}) = 3x_0 + 16z_0 \pmod{2^n}$$

is a solution to

$$x^4 \equiv A_0 + 16 \pmod{2^n},$$

so the theorem holds by the Principle of Mathematical Induction.

Corollary 6.1. The number of incongruent quartic residues modulo 2^n is 1 if $n = 1, 2, 3$, or 4, and $\frac{1}{8}\phi(2^n) = 2^{n-4}$ if $n \geq 5$.

Alternatively, Theorem 6 and its corollary can be shown by an approach that is more algebraic in spirit. The set of incongruent kth-power residues modulo m form a group $G_k(m)$ under modular multiplication. Corollary 2.1 states that $|G_2(2^n)| = 2^{n-3}$ if $n \geq 3$. The quartic residues must be found among the members of $G_2(2^n)$, and so by Lagrange's theorem [4] one has $|G_4(2^n)| = 2^k$, where the positive integer $k \leq n - 4$ because 9, for example, is always a quadratic residue modulo 2^n, but is never a quartic residue modulo 2^n.

The integer 17 is a quartic residue modulo 2^5. Assume that it is also a quartic residue modulo 2^n, that is, there are integers x_0, k_0 such that $x_0^4 - 17 = k_0 \cdot 2^n$. Now let $x = x_0 + 2^{n-2}K$, $x^4 \equiv 17 \pmod{2^{n+1}}$, with K to be determined. The congruence reduces to

$$x_0^3 K \equiv -k_0 \pmod{2},$$

which has a unique solution K_0 modulo 2. It follows by the Principle of Mathematical Induction that 17 is a quartic residue modulo 2^n for all $n \geq 5$.

The powers of 17 constitute a cyclic subgroup $H_4(2^n) \subseteq G_4(2^n)$. What we want to do is show that 17 generates all of $G_4(2^n)$.

Theorem 7. $|H_4(2^n)| = |G_4(2^n)| = 2^{n-4}$ if $n \geq 5$.

Proof. When $n = 5$, then

$$17^{2^{n-4}} \equiv 1 \pmod{2^n}$$

holds. Assume it also holds for $n = k$. Then

$$\begin{aligned} 17^{2^{k-3}} - 1 &= (17^{2^{k-4}})^2 - 1 \\ &= (17^{2^{k-4}} - 1)(17^{2^{k-4}} + 1) \end{aligned}$$

and as 2^k divides the first factor on the right by the induction hypothesis and 2 divides the second factor, then

$$17^{2^{k-3}} \equiv 1 \pmod{2^{k+1}}.$$

Hence, for any $n \geq 5$ the order of $H_4(2^n)$ does not exceed 2^{n-4}. The order of $H_4(2^n)$ must be a power of 2, but the power 2^{n-5} is too small. From the Binomial Theorem we have

$$\begin{aligned} (16+1)^{2^{n-5}} - 1 &= 16^{2^{n-5}} + 2^{n-5}(16)^{2^{n-5}-1} + \cdots + 2^{n-5}(16)^1 \\ &= 2^{2^{n-3}} + 2^{2^{n-3}+n-9} + \cdots + 2^{n-1}. \end{aligned}$$

Each term on the right except the last is divisible by 2^n, so

$$17^{2^{n-5}} \not\equiv 1 \pmod{2^n}$$

and $|H_4(2^n)| \not< 2^{n-4}$. It follows that $|H_4(2^n)| = 2^{n-4}$, and since $|G_4(2^n)|$ cannot exceed 2^{n-4}, it must be that $|H_4(2^n)| = |G_4(2^n)| = 2^{n-4}$ and the elements of $G_4(2^n)$ are the numbers indicated in Theorem 6.

Comparing Corollaries 2.1 and 6.1, we see that for $n \geq 5$ the number of incongruent quartic residues modulo 2^n is exactly half the number of incongruent quadratic residues modulo 2^n. A similar relationship was noted for moduli that are $(4k+1)$-primes [1]. It may be remarked that this relationship between the sets of quadratic and quartic residues is not general for arbitrary moduli. Thus, the modulus 12 has identical sets of incongruent quadratic and quartic residues, namely, the singleton set $\{1\}$.

References

1. J. B. Dence and T. P. Dence, "Cubic and Quartic Residues Modulo a Prime," *Missouri Journal of Mathematical Sciences*, 7 (1995), 24–31.

2. T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, New York, (1951), 115.

3. K. H. Rosen, *Elementary Number Theory and its Applications*, 3rd ed., Addison-Wesley, Reading, Massachusetts, (1993), 307.

4. J. B. Fraleigh, *A First Course in Abstract Algebra*, 5th ed., Addison-Wesley, Reading, Massachusetts, (1994), 121.

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

æ