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 $x^2 \equiv A \pmod{2^7}$.