On The Characterization Of Primes With 2 As Quadratic Residue, Non-Residue

Anthony Browne

May 14, 2016

ABSTRACT

I introduce a congruence that restates the characterization of primes that have 2 as a quadratic residue, non-residue.

One can observe that,

$2^{\frac{p_{n-1}}{2}} - 1 \equiv mod\ p_n$ at exactly the position of the even numbers in $\frac{p_n^2-1}{24}$. For $2^{\frac{p_{n-1}}{2}} + 1$, it is the opposite. From this,

$$2^{\frac{p_{n-1}}{2}} - (-1)^{\frac{p_n^2-1}{24}} \equiv mod\ p_n \text{ for } p \geq 3.$$

This implies,

$$2^{\frac{n-1}{2}} - (-1)^{\frac{n^2-1}{24}} \equiv mod\ n \quad if \quad n \ \ is\ prime \quad \text{for } \ n \geq 5.$$

Which I will prove in the following theorem.

Theorem:

$$2^{\frac{n-1}{2}} - (-1)^{\frac{n^2-1}{24}} \equiv mod\ n \quad if \quad n \ \ is\ prime \qquad n \geq 5.$$

Proof:

Let n be a prime ≥ 5. There are two cases to examine.

Case 1:

If n is of the form $8k \mp 1$, than 2 is a quadratic residue of n. Therefore, $2^{\frac{n-1}{2}} \equiv 1\ (mod\ n)$. But if $n \equiv \mp 1(mod\ 8)$, then $\frac{n^2-1}{24}$ is even. Therefore, $(-1)^{\frac{n^2-1}{24}} = 1$. So the congruence holds in this case.

Case 2:

If n is of the form $8k \mp 3$, than 2 is a quadratic non-residue of n. Therefore,

$2^{\frac{n-1}{2}} \equiv -1\ (mod\ n)$. But if $n \equiv \mp 1(mod\ 8)$, then $\frac{n^2-1}{24}$ is odd. Therefore, $(-1)^{\frac{n^2-1}{24}} = -1$. So the congruence holds in this case. End Proof

Note: The proof of the theorem is not of the author's design and was provided by another.

This is a restatement on the characterization of primes that have 2 as a quadratic residue, non-residue. The congruence holds for some composites as well. As an example, the congruence holds for the Carmichael number 561.