A Clever Use for Congruences

Fermat’s (Little) Theorem says that if \( p \) is a prime number and \( a \) is any integer, then \( a^p \equiv a \mod p \).

As a consequence, we have the following:

**Lemma:** If \( p \) is a positive number and there is some integer \( a \) with \( a^p \not\equiv a \mod p \), then \( p \) is a composite number. If there is some positive integer \( a < p \) with \( a^{p-1} \not\equiv 1 \mod p \), then \( p \) is a composite number.

We can use this lemma to show certain numbers are composite. For example, let’s look at \( p = 1111 \) and use \( a = 2 \).

We can go even further and use exercise #24 from section 1.4: once we have an even power of \( a \) congruent to 1, say \( a^{2n} \equiv 1 \mod p \), is \( a^n \equiv \pm 1 \mod p \)?