

## A Clever Use for Congruences

Recall Fermat's (Little) Theorem:

**Theorem:** If  $p$  is a prime number and  $a$  is any integer, then  $a^p \equiv a \pmod{p}$ .

As a consequence, we have the following

**Lemma:** If  $p$  is a positive number and there is some integer  $a$  with  $a^p \not\equiv a \pmod{p}$ , then  $p$  is a composite number. If there is some integer  $a < p$  with  $a^{p-1} \not\equiv 1 \pmod{p}$ , 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  $a^{2n} \equiv 1 \pmod{p}$ , is  $a^n \equiv \pm 1 \pmod{p}$ ?