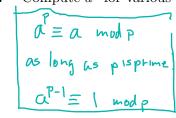
Powers mod Powers

Main Question: What is the remainder when you divide a^p by p?

Compute a^p for various values of a and p. What is your conjecture?



1. Compute
$$a^p$$
 for various values of a and p . What is your conjecture?

 $A^p \equiv a \mod p$

as long as pisptime

 $A^{p-1} \equiv 1 \mod p$
 $A^{p-1} \equiv 1 \mod p$

15 there some m s.t.

 $A^{m} \equiv 1 \mod 6$
 $A^{m} \equiv 1 \mod 6$
 $A^{m} \equiv 1 \mod 6$

Find the remainders when you perform the following divisions. Try different values of a.

- a^6 divided by 10?
- a^9 divided by 15?
- a^{13} divided by 21?
- as long as a 15 relatively prime to 2419.

Work
$$U(p) = \mathbb{Z}_p^* = \{1, 2, ..., p-1\}$$

multiplication mod p

In any group G, the order of an element
$$g \in G$$
 is the least $K>0$ such that $g^K = e$

$$\langle \alpha \rangle = \{ \alpha, \alpha^2, \alpha^3, \dots \}$$

$$2^3 = 1$$
 ord(2) = 3

$$|U(\rho)| = \rho - 1$$