Powers mod Powers

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

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

$\boxed{\begin{array}{l} a^p \equiv a \mod p \\ \text{as long as } p \text{ is prime} \\ a^{p-1} \equiv 1 \mod p \end{array}}$

$3^5 = 243 \equiv 3 \mod 5$

$3^4 = 81 \equiv 1 \mod 5$

$\times\ 2^6 = 64 \equiv 4 \mod 6$

is there some m s.t.

$2^m \equiv 1 \mod 6$?

$5^m \equiv 1 \mod 6$?

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

2. a^6 divided by 10?

3. a^9 divided by 15?

4. a^{13} divided by 21?

5. a^{2321} divided by 2419?

$\equiv 1 \mod 2419$

as long as a is relatively prime to 2419.

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

multiplication mod p

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

$$\underbrace{g, g^2, g^3, \ldots g^k = e}_{\text{different}}, \quad g^{k+1} = g$$

$|G|$ is called the order of G

$$\langle a \rangle = \{a, a^2, a^3, \ldots\}$$

$$|\langle a \rangle| = \mathrm{ord}(a)$$

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$2^3 = 1 \qquad \mathrm{ord}(2) = 3$

$\mathrm{ord}(1) = 1$

$\mathrm{ord}(3) = 6$

$\mathrm{ord}(4) = 3$

$\mathrm{ord}(5) = 6$

$\mathrm{ord}(6) = 2$

Lagrange's Theorem.

$|U(p)| = p - 1.$