Euler's Totient Function

In order to understand how internet encryption works, you need to understand the Totient function (more later....) and how to find a modular multiplicative inverse.

Modular Multiplicative Inverses:

The modular multiplicative inverse of an integer 'a', modulo 'm', is an integer x such that:

$$ax \equiv 1 \pmod{m}$$

For example, the multiplicative inverse of 7 (mod 3) is:

$$7x \equiv 1 \pmod{3}$$

so x = 1, or 4, or 7, or.....

Jan 18-10:34

However, multiplicative inverses only exist for certain combinations of 'a' and 'm'.

Choose some other values of 'a' and 'm' (keep them < 20) and try to determine the conditions for a multiplicative inverse to exist.

You may need to generate a fair amount of data, so careful group management may be required.

Jan 18-10:51

Euler's Totient Function, $\phi(n)$

$\phi(9) = 6$ $\phi(4) = 2$

$\phi(7) = 6$ $\phi(10) = 4$

$\phi(12) = 4$ $\phi(24) = 8$

Jan 18-11:04

Euler's Function (providing 'a' is coprime to 'n')

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Explore this relationship.

Jan 18-11:26

The theorem may be used to easily reduce large powers modulo *n*. For example, consider finding the last decimal digit of 7^{222}

ie $7^{222} \pmod{10}$

Note that 7 and 10 are coprime, and $\phi(10) = 4$.

So Euler's theorem yields .....?

and we get:

$7^{222} \equiv 7^{4\times55+2} \equiv (7^4)^{55} \times 7^2 \equiv 1^{55} \times 7^2 \equiv 49 \equiv 9 \pmod{10}$.

Jan 18-11:12