Euler's totient function (and Euler's theorem)

Last time, we explored multiplication and taking powers in modular (clockwork) arithmetic, and we ended with the following fact:

THM (Fermat's little theorem)

Let p be a prime number. If $a \not\equiv 0 \bmod p$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Q: This is the same as $a^p \equiv a \pmod{p}$. Why?

If you look back at the power tables we made last week, you will find that 1's appear a lot on the tables! More than just in the column corresponding to "p-1" on the $\mathbb{Z}/p\mathbb{Z}$ tables where p is prime. They occur other places in the table ... and on the $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ tables.

Brainstorm session: In what other places does a 1 appear on the table? Why does it appear? (Side question: what is special about 1 when it comes to multiplication?)

To best understand the appearance of some of the other 1's, we need to use the Euler totient function:

DEF Let m be a positive integer. The Euler totient function $\varphi(m)$ is the number of integers k with $1 \leq k \leq m$ such that $\gcd(k, m) = 1$

greatest common divisor of k and m.

Ex $\gcd(12, 36) =$

Ex $\gcd(6, 9) =$

Let's compute a few values of the Euler totient function.

$\varphi(1) =$

$\varphi(2) =$

$\varphi(3) =$

$\varphi(4) =$

$\varphi(5) =$

$\varphi(6) =$

$\varphi(7) =$

$\varphi(8) =$

Question: What patterns are you seeing?

Notice: peculiar that $\varphi(2) \cdot \varphi(3) = \varphi(2 \cdot 3)$ ... why is this happening?

"Proposition"

Prop 1 If p is prime, then the $\varphi(p) =$ ____.

Prop 2 If p is prime, and k is any positive integer,

then $\varphi(p^k) =$ _____.

Prop 3 If m, n are positive integers and $\gcd(m,n)=1$,

then $\varphi(m \cdot n) =$ _____.

Fun fact: Prop 2 and Prop 3 give us a way to compute $\varphi(m)$ for any m!

EXAMPLE Compute $\varphi(600)$.

Notice $600 = \underbrace{2^3 \cdot 3 \cdot 5^2}$ (check!)

"prime factorization"

We know: $\gcd(2,3)=1$, $\gcd(3,5)=1$, $\gcd(2,5)=1$ ...

and, in fact, $\gcd(2^3, 3\cdot 5^2)=1$, $\gcd(3,5^2)=1$...

why?

Now, try:

$\varphi(600) =$

Now, we can state a fact which helps us resolve the mystery of the 1's appearing in the power tables:

THM (Euler's Theorem)

Let m be a positive integer and a be an integer with $\gcd(a,m) = 1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Compare this to the power tables!

Challenge Problem: What are the last two digits of 3^{84}? Hint: The last two digits of 3^{84} are the same as the two digits of $3^{84} \pmod{100}$.