Example 1. Let a be an integer. Show a^{9^9} and a^9 have the same last two digits.

Proof. Our aim is to show that these two integers are congruent modulo:

Case 1. $a \perp 100$.

Then we calculate

$\phi(100) =$

Next, we find: $9^9 \equiv$

Then: $a^{9^9} =$

This is an application of the general Euler's Theorem corollary that if $a \perp n$ and:

then:

Case 2. Next let's consider the case that a is not $\perp 100$.

We can write a in the form

$a = 2^k \cdot 5^\ell \cdot b$ where:

We calculate

$a^{9^9} =$

$a^9 =$

Since $b \perp 100$, we already know from the first case that $b^{9^9} \equiv$

So, it remains to show that

goal $\to 2^{9^9} \equiv$

goal $\to 5^{9^9} \equiv$

or equivalently by dividing

goal $\to$

goal $\to$

In this form, note the base of the exponential expression and the modulus are:

so that Euler's theorem will apply.

Next we take the exponents modulo $\phi(25) = 20$ and $\phi(4) = 2$ to obtain

$9^9 - 2 \equiv$

$9^9 - 2 \equiv$

so that by Euler's theorem

$2^{9^9-2} \equiv$

$5^{9^9-2} \equiv$

A. **Phi and Convolutions.** We next prove results about ϕ and convolutions.

Theorem. $\phi * \mathbb{1} =$

In other words, for positive integers n, we have

$$\sum_{d|n} \phi(d) =$$

Proof. Both sides of the purported equality are:

Hence, we need only prove the equality for

Let p^k be a positive power of a prime.

Then

$(\phi * \mathbb{1})(p^k) =$

□

We can use the Möbius inversion formula to describe ϕ in terms of μ.

Theorem. $\phi =$

In other words, for positive integers n, we have

$\phi(n) =$

Proof. We use the theorem at the top of the page to write

$\mu * \mathrm{id} =$

and then using Möbius inversion, $\mu * \mathbb{1} = \epsilon$ where ϵ is the unit in convolutions

$\cdots =$

□

Let's illustrate the second theorem in the case that $n = 10$.

$\phi(10) =$

$$\sum_{d|10} \mu(d) \cdot \frac{10}{d} =$$

B. **Summing Invertible Residues.**

Theorem. Let n be an integer greater than 1.

If all the integers from $[1 \dots n]$ that are $\perp n$ are summed, the result is

Proof. We begin with a lemma.

Lemma. Let a be an integer. Then $a \perp n$ iff $(n - a) \perp n$.

Proof. This is clear, because, first, a negative does not change the gcd

$$\gcd(a, n) =$$

and second, because if $x \equiv y \mod n$ then:

$$\gcd(-a, n) =$$

□

Therefore, the list of integers of integers from $[1 \dots n]$ that are $\perp n$

can alternatively be enumerated as

If we add all these integers $\perp n$, but twice over, we get

Hence, dividing by two gives us the sum of these integers, and success.

□

For example, let's see the nature of this argument in the case $n = 10$.