# Math for CS 2015/2019 solutions to "In-Class Problems Week 6, Wed. (Session 14)"

https://github.com/spamegg1

October 26, 2022

## Contents



## 1 Problem 1

Find the remainder of $26^{1818181}$ divided by 297.

Hint: $1818181 = (180 \cdot 10101) + 1$; use Euler's theorem.

*Proof.* 1.First we notice that $297 = 3^3 \cdot 11$, and therefore (using Problem 3)

$$\phi(297) = \phi(3^3 \cdot 11) = (3^3 - 3^2)(11 - 1) = 18 \cdot 10 = 180$$

So you see it's not a coincidence that the Hint mentions the number 180.

2. Also notice that $26 = 2 \cdot 13$ is relatively prime to $297 = 3^3 \cdot 11$. Therefore by Euler's Theorem: $26^{\phi(297)} = 26^{180} \equiv 1 \mod 297$.

3. Using the hint we get

$$26^{1818181} = 26^{(180 \cdot 10101)+1} = 26^{180 \cdot 10101} \cdot 26 = (26^{180})^{10101} \cdot 26$$

4. By (2) $26^{180} \equiv 1 \mod 297$ therefore $(26^{180})^{10101} \equiv 1 \mod 297$.
5. So by (4) $(26^{180})^{10101} \cdot 26 \equiv 26 \mod 297$.
6. By (3) and (5) the remainder we are looking for is 26.

□

# 2 Problem 2

## 2.1 (a)

Prove that $2012^{1200}$ has a multiplicative inverse modulo 77.

*Proof.* We notice that $2012 = 2^2 \cdot 503$ is relatively prime to $77 = 7 \cdot 11$. Therefore $2012^{1200}$ has a multiplicative inverse modulo 77. □

## 2.2 (b)

What is the value of $\phi(77)$, where $\phi$ is Euler's function?

*Proof.*

$$\phi(7 \cdot 11) = (7-1)(11-1) = 6 \cdot 10 = 60$$

□

## 2.3 (c)

What is the remainder of $2012^{1200}$ divided by 77?

*Proof.* By Euler's Theorem and part (a):

$$2012^{1200} = 2012^{60 \cdot 20} = (2012^{60})^{20} = (2012^{\phi(77)})^{20} \equiv 1^{20} \equiv 1 \mod 77$$

□

# 3 Problem 3

Prove that for any prime, $p$, and integer, $k \geq 1$,

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

where $\phi$ is Euler's function.

Hint: Which numbers between 0 and $p^k - 1$ are divisible by $p$? How many are there?

Note: This is proved in the text. Don't look up that proof.

*Proof.* The proof is by induction on $k$. The statement we want to prove is: for $k \geq 1$

$$P(k) ::= \phi(p^k) = p^k - p^{k-1}$$

**Base case:** $k = 1$. The numbers $1, 2, 3, \ldots, p-1$ are all relatively prime to $p$. There are $p-1$ such numbers. Therefore $\phi(p^1) = p^1 - 1$ which proves $P(1)$.

**Induction Step.**

1. Assume $P(k)$ is true. We want to prove $P(k+1)$.

2. The numbers that are relatively prime to $p^{k+1}$ can be divided into two sets:

(I). The numbers in the interval $[0, p^k]$ that are relatively prime to $p^{k+1}$,

(II). The numbers in the interval $[p^k, p^{k+1}]$ that are relatively prime to $p^{k+1}$.

3. By the Induction Hypothesis, the number of numbers relatively prime to $p^{k+1}$ in the set (I) is $p^k - p^{k-1}$.

4. Let's consider the set (II). Consider the interval $[p^k, p^{k+1}]$. This can be divided up into $p-1$ subintervals, each of length $p^k$:

$$[p^k, p^k \cdot 2], [p^k \cdot 2, p^k \cdot 3], \ldots, [p^k \cdot (p-1), p^k \cdot p]$$

5. Each one of these subintervals is the same as $[0, p^k]$ except they are shifted by a multiple of $p^k$. So each one of these subintervals contain exactly the same number of multiples of $p$ as does the interval $[0, p^k]$.

6. By (5), each one of these subintervals contain exactly the same number of numbers relatively prime to $p^{k+1}$ as does the interval $[0, p^k]$.

6. So, by (6) and by the Induction Hypothesis, for each one of these subintervals, the number of numbers relatively prime to $p^{k+1}$ in that interval is $p^k - p^{k-1}$.

7. There are $p-1$ such subintervals, so the total count of numbers that are relatively prime to $p^{k+1}$ is:

$$\begin{gathered} p^k - p^{k-1} \text{ (from the interval } [0, p^k]) \\ (p-1)(p^k - p^{k-1}) \text{ (from the } p-1 \text{ subintervals of } [p^k, p^{k+1}]) \\ p(p^k - p^{k-1}) \text{ (total in the interval } [0, p^{k+1}]) \end{gathered}$$

8. Since $p(p^k - p^{k-1}) = p^{k+1} - p^k$, this proves $P(k+1)$.

This completes the induction, so we have proved $\phi(p^k) = p^k - p^{k-1}$ for all $k \geq 1$. $\square$

# 4 Problem 4

At one time, the Guinness Book of World Records reported that the "greatest human calculator" was a guy who could compute 13th roots of 100-digit numbers that were 13th powers. What a curious choice of tasks.

In this problem, we prove (1): $n^{13} \equiv n \mod 10$ for all $n$.

## 4.1 (a)

Explain why (1) does not follow immediately from Euler's Theorem.

*Proof.* It is true that $\phi(10) = \phi(2)\phi(5) = (2-1)(5-1) = 4$, so for any $n$ that is relatively prime to 10, we have $n^4 \equiv 1 \mod 10$. So $n^{12} = (n^4)^3 \equiv 1^3 \mod 10$. Then multiply this by $n$ to get $n^{13} \equiv n \mod 10$.

But this only works if $n$ is relatively prime to 10. □

## 4.2 (b)

Prove that $d^{13} \equiv d \mod 10$ for $0 \leq d < 10$.

*Proof.* By the above argument in part (a), this is true for $d$ that is relatively prime to 10, that is, this is true for $d = 1, 3, 7, 9$. Let's manually check the others.

$d = 0$: $0^{13} = 0 \equiv 0 \mod 10$.

$d = 2$: $2^{13} = 8192 \equiv 2 \mod 10$.

$d = 4$: $4^{13} = 2^{26} = (2^{13})^2 \equiv 2^2 \equiv 4 \mod 10$. (Here we are using the case $d = 2$ from above.)

$d = 5$: $5^{13} \equiv 5 \mod 10$ because any multiple of 5 ends with 5 as its last digit, so its remainder when divided by 10 will always be 5. (This is true for any power, not just 13.)

$d = 6$: $6^{13} = (2 \cdot 3)^{13} = 2^{13} \cdot 3^{13} \equiv 2 \cdot 3 \equiv 6 \mod 10$. (Here we are using the cases $d = 2$ and $d = 3$ from above.)

$d = 8$: $8^{13} = 2^{39} = (2^{13})^3 \equiv 2^3 \equiv 8 \mod 10$. (Here we are using the case $d = 2$ from above.) □

## 4.3 (c)

Now prove the congruence (1).

*Proof.* 1. There exist integers $m, k$ such that $n = 10k + d$ where $0 \leq d < 10$.

2. Then $n \equiv d \mod 10$. So $n^{13} \equiv d^{13} \mod 10$.

3. By part (b) we have $d^{13} \equiv d \mod 10$.

4. By (2) and (3), $n^{13} \equiv d \mod 10$.

5. By (4) and (2), $n^{13} \equiv n \mod 10$. □