CS 70: Homework #4

Abhijay Bhatnagar

September 21, 2018

Problem 1: Modular Arithmetic Solutions

Find all solutions (modulo the corresponding modulus) to the following equations. Prove that there are no other solutions (in a modular setting) to each equation.

(a) $2x \equiv 5 \pmod{15}$

Solution: 10, which is unique modulo 15.

Proof. The inverse of 2 (mod 15) is 8 ($2 \cdot 8 = 16 = 1 \bmod 15$). From there, we solve the original equation:

$$\begin{aligned} 2 \cdot 2^{-1} \pmod{15} &= 5 \cdot 2^{-1} \pmod{15} \\ &= 5 \cdot 8 \pmod{15} \\ &= 40 \pmod{15} \\ &= 10 \pmod{15} \end{aligned}$$

□

(b) $2x \equiv 5 \pmod{16}$

Solution: No solution. 2 and 16 are not relatively prime, therefore $2x \equiv 5 \pmod{16} \implies 2x \equiv 1 \pmod{2}$, which has no solution, therefore the former equation is also inconsistent.

(c) $5x \equiv 10 \pmod{25}$

Solution: 2, 7, 12, 17, and 22 (which are unique modulo 15).

Proof. All three numbers are divisible by 5, therefore the original equation implies

$$x \equiv 2 \pmod{5}$$

From there, we solve the equation using ($1^{-1} \pmod{5} = 6$):

$$\begin{aligned} 1 \cdot 1^{-1} \pmod{5} &= 2 \cdot 1^{-1} \pmod{5} \\ &= 2 \cdot 6 \pmod{5} \\ &= 12 \pmod{5} \\ &= 2 \pmod{5} \end{aligned}$$

Which is equivalent to {2, 7, 12, 17, 22} modulo 25. □

Problem 2: Euclid's Algorithm

(a) Use Euclid's algorithm from lecture to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

Solution: 17.

x	y
527	324
323	204
204	119
119	85
85	34
34	17
17	0

(b) Use extended Euclid's algorithm from lecture to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

Solution: 11.

x	y		d	a	b
27	5		1	-2	11
5	2	$\Longrightarrow$	1	1	-2
2	1		1	0	1
1	0		1	1	0

From the extended Euclid's algorithm, we know: $1 = -2(27)+11(5) \implies 5^{-1} \pmod{27} = 11$.

(c) Find $x \pmod{27}$ if $5x + 26 \equiv 3 \pmod{27}$. You can use the result computed in (b).

Solution: 17 (mod 27).

$$\begin{aligned} 5x + 26 &\equiv 3 \pmod{27} \\ 5x &\equiv -23 \pmod{27} \\ 5x &\equiv 4 \pmod{27} \\ x &\equiv 4 \cdot 11 \pmod{27} \\ x &\equiv 17 \pmod{27} \end{aligned}$$

(d) Assume a, b, and c are integers and $c > 0$. Prove or disprove: If a has no multiplicative inverse mod c, then $ax \equiv b \pmod{c}$ has no solution.

Solution: False. Consider the equation $5x \equiv 10 \pmod{25}$. 5 has no multiplicative inverse mod 25. However, $x = 2$ is a solution.

Problem 3: Modular Exponentiation

Compute the following:

(a) $13^{2018} \pmod{12}$

Solution: 1.

$$\begin{aligned} 13^1 &= 1 \pmod{12} \\ 13^2 &= 1 \pmod{12} \\ &\dots \\ 13^{2018} &= \text{some product of ones} \pmod{12} \\ &= 1 \pmod{12} \end{aligned}$$

(b) $8^{11111} \pmod{9}$

Solution: 8 (mod 9).

$$\begin{aligned} 8^1 &= 8 \pmod{9} \\ 8^2 &= 1 \pmod{9} \\ 8^4 &= 1 \pmod{9} \\ &\dots \\ 8^{11111} &= 8^1 \cdot (8^2)^{5555} \pmod{9} \\ &= 8 \cdot 1 \pmod{9} \\ &= 8 \pmod{9} \end{aligned}$$

(c) $7^{256} \pmod{11}$

Solution: 4 (mod 11).

$$\begin{aligned} 7^1 &= 7 \pmod{11} \\ 7^2 &= 5 \pmod{11} \\ 7^4 &= 3 \pmod{11} \\ 7^8 &= 9 \pmod{11} \\ 7^{16} &= 4 \pmod{11} \\ 7^{32} &= 5 \pmod{11} \\ &\dots \\ 7^{256} &= (7^{32})^{2^3} \pmod{11} \\ &= (7^2)^{2^3} \pmod{11} \text{ (because it repeats)} \\ &= (7^{16}) \pmod{11} \\ &= 4 \pmod{11} \end{aligned}$$

(d) $3^{160} \pmod{23}$

Solution: 16 (mod 23).

$$\begin{aligned}
3^1 &= 3 \pmod{23} \\
3^2 &= 9 \pmod{23} \\
3^4 &= 12 \pmod{23} \\
3^8 &= 6 \pmod{23} \\
3^{16} &= 13 \pmod{23} \\
3^{32} &= 8 \pmod{23} \\
3^{64} &= 18 \pmod{23} \\
3^{128} &= 2 \pmod{23}
\end{aligned}$$

$$\begin{aligned}
\therefore 3^{160} &= 3^{128} \cdot 3^{32} \pmod{23} \\
&= 2 \cdot 8 \pmod{23} \\
&= 16 \pmod{23}
\end{aligned}$$

Problem 4: Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \texttt{gcd}(n, i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m, n such that $\texttt{gcd}(m, n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

Solution: $p - 1$

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

Solution: $p^k - p^{k-1}$ [Alternatively: $(p-1)p^{k-1}$]

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod p$? *(Hint: use Fermat's Little Theorem.)*

Solution: $1 \pmod p$.

Proof.

$$\begin{aligned} a^{\phi(p)} \pmod p &\equiv a^{p-1} \pmod p \\ &\equiv (a^p/a) \pmod p \\ &\quad \text{Using Fermat's Little Theorem..} \\ &\equiv a/a \pmod p \\ &\equiv 1 \pmod p \end{aligned}$$

□

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1, 2, \ldots, k\}, \;\; a^{\phi(b)} \equiv 1 \pmod{p_i}$$

Solution:

Proof.

$$b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k} \tag{1}$$
$$\phi(b) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k}) \tag{2}$$
$$\phi(b) = (p_1 - 1)(p_1^{\alpha_1 - 1}) \cdot (p_2 - 1)(p_2^{\alpha_2 - 1}) \ldots (p_k - 1)(p_k^{\alpha_k - 1}) \tag{3}$$

From here, we want to convert $\phi(b)$ into a form we can use with our extension to Fermat's Little Theorem from part (c). More specifically we want to isolate the $(p_i - 1)$ term.

Conveniently, all of the terms in (3) are natural numbers, therefore we can rewrite all other terms of (3) as a product of constants:

$$\phi(b) = (p_i - 1) \cdot \prod_j c_j \tag{4}$$
$$= (p_i - 1) \cdot c \tag{5}$$

From (5), we can solve for $a^{\phi(b)} \pmod{p_i}$:

$$a^{\phi(b)} \equiv a^{(p_i - 1) \cdot c} \pmod{p_i} \tag{6}$$
$$\equiv (a^{p_i - 1} \pmod{p_i})^c \tag{7}$$
$$\equiv 1^c \pmod{p_i} \tag{8}$$
$$\equiv 1 \pmod{p_i} \tag{9}$$

This works for any arbitrary p_i, therefore the initial statement holds. □

Problem 5: FLT Converse

Recall that the FLT states that, given a prime n, $a^{n-1} \equiv 1 \pmod{n}$ *for all* $1 \leq a \leq n-1$. Note that it says nothing about when n is composite.

Can the FLT condition ($a^{n-1} \equiv 1 \mod n$) hold for some or even all a if n is composite? This problem will investigate both possibilities. It turns out that unlike in the prime case, we need to restrict ourselves to looking at a that are relatively prime to n. (Note that if n is prime, then every $a < n$ is relatively prime to n). Because of this restriction, let's define

$$S(n) = \{i : 1 \leq i \leq n, \texttt{gcd}(n, i) = 1\},$$

so $\mid S \mid$ is the total number of possible choices for a.

(a) Prove that for every a and n that are not relatively prime, FLT condition fails. In other words, for every a and n such that $\texttt{gcd}(n, a) \neq 1$, we have $a^{n-1} \not\equiv 1 \pmod{n}$.

Solution:

Proof. $a^{n-1} \equiv 1 \pmod{n} \iff \exists x : a^{n-1}x \equiv 1 \pmod{n} \iff a^{n-1}$ has an inverse $\pmod{n}$. Since we know n and a are not relatively prime, we also know $\texttt{gcd}(n, a^{n-1}) \neq 1$ (the prime factorization of a^{n-1} would contain the same common prime factor of n and a). From there, we know from Theorem 6.2 that a^{n-1} has no inverse, therefore $a^{n-1} \not\equiv 1 \pmod{n}$ □

(b) Prove that the FLT condition fails for most choices of a and n. More precisely, show that if we can find a single $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, we can find at least $|S(n)|/2$ such a. (Hint: You're almost there if you can show that the set of numbers that fail the FLT condition is at least as large as the set of numbers that pass it. A clever bijection may be useful to compare set sizes.)

Solution:

The above tells us that if a composite number fails the FLT condition for even one number relatively prime to it, then it fails the condition for most numbers relatively prime to it. However, it doesn't rule out the possibility that some composite number n satisifes the FLT condition entirely: *for all* a relatively prime to n, $a^{n-1} \equiv 1 \mod n$. It turns out such numbers do exist, but they were found through trial-and-error! We will prove one of the conditions on n that make it easy to verify the existence of these numbers.

c.) First, show that if $a \equiv b \mod m_1$ and $a \equiv b \mod m_2$, with $\gcd(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 m_2}$.

Solution:

Proof. Starting from the givens:

$$a \equiv b \mod m_1 \implies m_1 | (b - a)$$
$$a \equiv b \mod m_2 \implies m_2 | (b - a)$$

From here, we can proceed by contradiction.

If $a \not\equiv b \pmod{m_1 m_2}$, then $m_1 m_2 \not| (b-a)$

$\implies b - a = m_1 m_2 k + r$ (where $k \in \mathbb{Z}$ and $r \in \mathbb{Z}^+, r < m_1 m_2$)

$\implies r = (b-a) - m_1 m_2 k$

Now we know $m_1 | (b-a)$ and $m_2 | (b-a) \implies r = m_1 c_1 - m_1 m_2 k$ and $r = m_2 c_2 - m_1 m_2 k$ for some c_1, c_2. This implies $m_1 | r$ and $m_2 | r$. Since $\gcd(m_1, m_2) = 1$, the lowest number that is divisible by both is $m_1 m_2$. However, we know $r < m_1 m_2$, therefore we have a contradiction as desired. □

d.) Let $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $p_i - 1 \mid n - 1$ for all i. Show that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$

Solution:

Proof. Starting from the given:

$a \in S(n) \implies gcd(a, n) = 1$.

For an arbitrary $p_i, a^{n-1} \equiv 1 \pmod{p_i}$ (from: $p_i - 1 \mid n - 1$).

From (c), this implies $a^{n-1} \equiv 1 \pmod{p_1 p_2 ... p_k} \equiv 1 \pmod{n}$ □

e.) Verify that for all a coprime with 561, $a^{560} \equiv 1 \pmod{561}$.

Solution: If we can verify $p_i - 1 \mid 561 - 1$ for all prime factors of 561, then from (d) we know $a^{560} \equiv 1 \pmod{561}$ for all a coprime with 561.

Prime factors of 561 = {3, 11, 17}

$(2|560) \wedge (10|560) \wedge (16|560) \implies a^{560} \equiv 1 \pmod{561}$ for all a coprime with 561.