CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

HW 4

Due: September 21, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

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

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

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

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.

(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.

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

(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.

3 Modular Exponentiation

Compute the following:

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

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

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

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

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 $\phi(p)$?

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

(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.)*

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

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

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

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 $|\,S\,|$ 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 $a^{n-1} \not\equiv 1 \pmod{n}$.

(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.)

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 $a \equiv b \pmod{m_1 m_2}$.

(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 $a \in S(n)$

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