CS 70 Discrete Mathematics and Probability Theory
Spring 2018 Satish Rao and Babak Ayazifar

HW 4

Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

1 Solution for $ax \equiv b \pmod{m}$

In the notes, we proved that when $\gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \pmod{m}$ has exactly one solution x (modulo m). This proof also implies that when $\gcd(m,a) = 1$, there is a unique solution to $ax \equiv b \pmod{m}$, where x is the unknown variable.

Now consider the equation $ax \equiv b \pmod{m}$, when $\gcd(m,a) > 1$.

(a) Let $\gcd(m,a) = d$. Prove that $ax \equiv b \pmod{m}$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \pmod{d}$. (Hint: If $b \equiv 0 \pmod{d}$, we can get a useful equation by dividing the equation $ax \equiv b \pmod{m}$ by d.)

(b) Let $\gcd(m,a) = d$. Assume $b \equiv 0 \pmod{d}$. Prove that $ax \equiv b \pmod{m}$ has exactly d solutions (modulo m).

(c) Solve for x: $77x \equiv 35 \pmod{42}$.

2 CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations $\mod 385$). Solve the system using the Chinese Remainder Theorem. What is $3^{302} \mod 385$?

3 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 number 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:

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

4 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. Unlike in the prime case, we need to restrict ourselves to looking at a that are 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) First, let's show the FLT condition breaks 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: Find a bijection that helps you bound the number of values that pass the FLT condition, and remember we only care about values in the set S)

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.

(b) 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 $a \equiv b \mod m_1 m_2$.

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

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