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.

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. (*signature here*)

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: $77x \equiv 35 \pmod{42}$.

Solution:

(a) **Necessary condition:** $ax \equiv b \pmod{m}$ has a solution $\implies b \equiv 0 \pmod{d}$.

If $ax \equiv b \pmod{m}$ has a solution, we can write $ax = my + b$ for some $x, y \in \mathbb{Z}$.
Since d is the greatest common divisor of m and a, we know that $d \mid a$ and $d \mid m$. Therefore d divides $ax - my = b$, or equivalently, $b \equiv 0 \pmod{d}$.

Sufficient condition: $b \equiv 0 \pmod{d} \implies ax \equiv b \pmod{m}$ has a solution.

Consider the congruent equation

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \tag{1}$$

We know that

$$\gcd(m,a) = d \implies \gcd\left(\frac{m}{d}, \frac{a}{d}\right) = 1.$$

Therefore (1) has a solution, or equivalently, $\exists x, y \in \mathbb{Z}$, such that

$$\frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}.$$

$\implies ax = my + b.$
$\implies x$ is a solution for $ax \equiv b \pmod{m}$.

Alternate proof for sufficient condition:

If $d \mid b$, we can write $b = kd$ for some $k \in \mathbb{Z}$. Since $\gcd(m,a) = d$, $\exists w, y \in \mathbb{Z}$, such that $aw + my = d$, similar to what we've seen with extended Euclid's algorithm. Multiplying both sides by k, we get $kaw + kmy = kd = b$. So

$$\begin{aligned} akw + mky &\equiv b \pmod{m}, \\ akw &\equiv b \pmod{m}. \end{aligned}$$

Then, kw is a solution of $ax \equiv b \pmod{m}$.

(b) From the proof of sufficient condition in Part (a), we have shown that if x satisfies (1), then x also satisfies $ax \equiv b \pmod{m}$. How about the reverse?
If x satisfies $ax \equiv b \pmod{m}$, then

$$\begin{aligned} & ax = my + b \text{ for some } y \in \mathbb{Z}, \\ \implies & \frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}, \\ \implies & x \text{ satisfies } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \end{aligned}$$

We conclude the following Lemma from the above proof:

Lemma: $\forall x \in \mathbb{Z}$, x satisfies (1) if and only if x satisfies $ax \equiv b \pmod{m}$.

Let x_0 be the unique solution of (1). For more general $x \in \mathbb{Z}$ that satisfies (1) must be of the form

$$x = x_0 + k\frac{m}{d} \qquad \text{for some } k \in \mathbb{Z}. \tag{2}$$

By the above Lemma, any $x \in \mathbb{Z}$ that satisfies $ax \equiv b \pmod{m}$ will also be of the form (2).

Now we will show that there are only d distinct solutions (modulo m) for $ax \equiv b \pmod{m}$ of the form (2). Two solutions,

$$x_1 = x_0 + k_1\frac{m}{d}$$
$$x_2 = x_0 + k_2\frac{m}{d}$$

are the same in modulo m if and only if

$$\begin{aligned} x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \pmod{m} &\iff (k_1 - k_2)\frac{m}{d} \equiv 0 \pmod{m}, \\ &\iff (k_1 - k_2)\frac{m}{d} = qm \text{ for some } q \in \mathbb{Z}, \\ &\iff (k_1 - k_2)m = qmd, \\ &\iff k_1 - k_2 = qd. \end{aligned}$$

The above argument proved that two solutions with the form (2) are equal $\pmod{m}$ if and only if $k_1 \equiv k_2 \pmod{d}$. Without loss of generality, we can construct solutions by letting $k \in \{0, 1, \ldots, d-1\}$. To be very specific, the d distinct solutions of $ax \equiv b \pmod{m}$ are

$$x \equiv x_0 + k\frac{m}{d} \pmod{m}, \qquad k = 0, 1, \ldots, d-1.$$

(c) Since $\gcd(77, 42) = 7$ and $35 \equiv 0 \pmod{7}$, we can find a unique solution from $(77/7)x \equiv 35/7 \pmod{42/7}$:

$$\begin{aligned} 11x &\equiv 5 \pmod{6} \\ -1x &\equiv -1 \pmod{6} \qquad \text{(because } 11 \equiv -1 \pmod{6} \text{ and } 5 \equiv -1 \pmod{6}\text{)} \\ x &\equiv 1 \pmod{6} \end{aligned}$$

The solution of $(77/7)x \equiv 35/7 \pmod{42/7}$ is $x \equiv 1 \pmod{6}$. Based on Part (b), the solutions of $77x \equiv 35 \pmod{42}$ are

$$x \equiv 1 + 6k \pmod{42}, \qquad k = 0, 1, \ldots, 6.$$

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 $3^{302} \mod 385$?

Solution:

(a) $385 = 11 \times 7 \times 5$.

(b) Since $3^4 \equiv 1 \pmod 5$, $3^{302} \equiv 3^{4(75)} \cdot 3^2 \equiv 4 \pmod 5$.
Since $3^6 \equiv 1 \pmod 7$, $3^{302} \equiv 3^{6(50)} \cdot 3^2 \equiv 2 \pmod 7$.
Since $3^{10} \equiv 1 \pmod{11}$, $3^{302} \equiv 3^{10(30)} \cdot 3^2 \equiv 9 \pmod{11}$.

(c) $x \equiv 4 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 9 \pmod{11}$.
The answer we get using CRT is $x \equiv 9 \pmod{385}$. So $3^{302} \equiv 9 \pmod{385}$.

3 Euler's Totient Function

Euler's totient function is defined as follows:

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

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 $\gcd(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(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:

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

Solution:

(a) Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.
So, $\phi(p) = p - 1$.

(b) The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.

The total number of positive integers less than or equal to p^k is p^k.

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

(c) From Fermat's Little Theorem, and part 1,

$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$

(d) From the property of the totient function and part 3:

$$\begin{aligned}\phi(b) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1)\end{aligned}$$

This shows that, for every p_i, which is a prime factor of b, we can write $\phi(b) = c \cdot (p_i - 1)$, where c is some constant. Since a and b are relatively prime, a is also relatively prime with p_i. From Fermat's Little Theorem:

$a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$

Since we picked p_i arbitrarily from the set of prime factors of b, this holds for all such 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, $a^{560} \equiv 1 \mod 561$.

Solution:

(a) The key to this argument is that we've already found one a that breaks the FLT condition. Let N_f be the set of integers coprime with n that fail the FLT condition, and N_p be the set of integers coprime with n that pass it. Note that $N_f \cup N_p = S(n)$, so $\mid N_f \mid + \mid N_p \mid = \mid S(n) \mid$. Therefore, our goal is to show that $|N_f| \geq |N_p|$, so that $|N_p| < \frac{S(n)}{2}$ immediately follows.

Assume there's another number b for which $b^{n-1} \equiv 1 \mod n$, i.e. $b \in N_p$. Consider $(a \cdot b)^{n-1} = a^{n-1} b^{n-1} = a^{n-1} \not\equiv 1 \mod n$, by assumption. So, given any b that satisfies the FLT condition, we can construct a number ab that breaks it! But is $ab \mod n$ unique? Yes, because $ax \mod n$ is a bijection, since $\gcd(a, n) = 1$. So for every $b \in N_p$, $ab \in N_f$, and $\mid N_p \mid \leq \mid N_f \mid$.

(b) This is a specialized version of the CRT where we can combine the moduli without calculating inverses. If $a = b \mod m_1$, then $a = km_1 + b$ for some k in $\mathbb{Z}$. If $a = b \mod m_2$, then $a = lm_2 + b$ for some $l \in \mathbb{Z}$. We want to relate the two moduli, so rewrite this as $a - b = lm_2$ and $a - b = km_1$, or $lm_2 = km_1$. Since m_1 and m_2 are coprime, $m_1 \mid l \implies l = dm_1$ for some $d \in \mathbb{Z}$. Substituting back in, we find $lm_2 = dm_1 m_2 \implies a - b = dm_1 m_2$. So, $a = b \mod m_1 m_2$.

(c) Since p_i are prime, we know that $a^{p_i - 1} = 1 \mod p_i$. Since $p_i - 1 \mid n - 1$, $a^{n-1} = a^{j(p_i - 1)} = (a^{p_i - 1})^j = 1 \mod p_i$. This holds for all a coprime with p_i. Thus, if we restrict ourselves to a that are coprime with all p_i, we have a set of k equations $a^{n-1} = 1 \mod p_i$. By the last part, we can conclude $a^{n-1} = 1 \mod n$, for any a that is coprime with all of the p_i. This condition is the same as a coprime with n, so we've shown n passes the FLT condition for "primality".

(d) $561 = 3 \times 11 \times 17$, and $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$. By the above condition, 561 passes the FLT test.