CS 70 Discrete Mathematics and Probability Theory
Fall 2024 Rao, Hug **HW 04**

Due: Saturday, 9/28, 4:00 PM
Grace period until Saturday, 9/28, 6:00 PM

Sundry

Before you start writing your final homework submission, 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.)

Solution: I worked with Lawrence Rhee (lawrencejrhee@berkeley.edu). We discussed our approaches to each problem and asked each other questions.

1 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y. For each subpart, show your work and justify your answers.

(a) $9x+5 \equiv 7 \pmod{13}$.

(b) Show that $3x+12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x+4y \equiv 0 \pmod 7$ and $2x+y \equiv 4 \pmod 7$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

Solution:

(a)

$$9x+5 \equiv 7 \pmod{13}$$
$$9x \equiv 2 \pmod{13}$$

Find modular inverse of 9 via trial and error.

$$9*3 \equiv 27 \equiv 1 \pmod{13}$$

Then

$$9*3*2 \equiv 2 \pmod{13}$$

Thus, $x = 6 \pmod{13}$.

(b) Suppose the equation does have a solution. Then, $3x+12 = 21y+4$ for some integer y. Then,

$$3x+12 \equiv 0 \pmod 3$$

and

$$21y+4 \equiv 1 \pmod 3.$$

This is a contradiction, since this implies LHS is not equal to RHS. Thus, there is no solution.

(c) Subtracting the 2nd equation 4 times from the first we get

$$-3x \equiv -16 \pmod 7$$

$$3x \equiv 2 \pmod 7$$

Since these are small numbers, we use trial and error to find that $x = 3$ works. Now, plugging in $x = 3$ to the first equation we get

$$15+4y \equiv 0 \pmod 7$$

$$4y \equiv 6 \pmod 7$$

Again, by trial and error we see that

$$4*5 = 20 \equiv 6 \pmod 7$$

as desired. Thus, $x = 3 \pmod 7, y = 5 \pmod 7$ is our solution. We can easily verify this:

$$5*3+4*5 = 35 \equiv 0 \pmod 7$$

$$2*3+5 = 11 \equiv 4 \pmod 7$$

(d) We know that

$$13^{2023} \equiv (13 \pmod{12})^{2023} \equiv 1^{2023} \equiv 1 \pmod{12}$$

Thus, $x = 1$ is our solution.

(e) By fermat's little theorem, we have that

$$7^{10} \equiv 1 \pmod{11}$$

Then,

$$7^{62} \equiv (7^{10})^6 7^2 \equiv 1*7^2 \equiv 49 \equiv 5 \pmod{11}$$

Thus, $x = 5$ is our solution.

2 Short Answer: Modular Arithmetic

Note 6

For each subpart, show your work and justify your answers.

(a) What is the multiplicative inverse of $n-1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x \equiv 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n \equiv 2 \pmod 3$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 \equiv 10 \pmod m$? (Answer should be an expression that is interpreted $\pmod m$, and shouldn't consist of fractions.)

Solution:

(a)

$$\begin{aligned} a(n-1) &\equiv 1 \pmod n \\ an - a &\equiv 1 \pmod n \\ -a &\equiv 1 \pmod n \\ a &\equiv -1 \pmod n \end{aligned}$$

Thus, $n-1$ is the multiplicative inverse of $n-1$ mod n.

(b) It is easy to see that

$$3 * 2 = 6 \equiv 6 \pmod{17}$$

Thus, $x = 2 \pmod{17}$ is the solution.

(c) We claim that this statement is true.
(Base case 1) let $n = 1$. It is given that $R_1 = 2$, thus works.
(Base case 2) let $n = 2$. We compute $R_2 = 4 * 2 - 3 * 0 = 8 \equiv 2 \pmod 3$, thus works.
(Hypothesis) suppose for all $n \in 1, \ldots, k$, $R_n \equiv 2 \pmod 3$.
(Step) Then, $R_{k+1} = 4R_k - 3R_{k-1} \equiv 4(2) - 3(2) \equiv 2 \pmod 3$.
Thus, by induction, $R_n \equiv \pmod 3$ for all $n \geq 1$.

(d) Taking the first equation mod m we have that

$$7 * 53 \equiv 1 \pmod m$$

Thus, 7 is the multiplicative inverse of 53.
We have

$$\begin{aligned} 53x + 3 &\equiv 10 \mod m \\ 53x &\equiv 7 \mod m \end{aligned}$$

Since we know the multiplicative inverse:

$$53 * 7 * 7 \equiv 1 * 7 \equiv 7 \pmod m$$

Thus, $x = 49 \pmod m$ is our solution.

3 Wilson's Theorem

Note 6 Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

Solution:

(a) (=>) Suppose p is prime. We have $(p-1)! = 1 * 2 * \cdots * (p-1)$. Let k be one of the factors in $1, 2, \cdots, (p-1)$. Since p is prime, $\gcd(k, p) = 1$. Then each k has a unique modular inverse modulo p. For some of the k's, their modular inverse is themself.

$$k^2 \equiv 1 \pmod{p}$$

$$k^2 - 1 \equiv 0 \pmod{p}$$

$$(k+1)(k-1) \equiv 0 \pmod{p}$$

Then, k is either 1 or $p-1$.
Let a_1 be one of the factors in $2, \cdots, (p-1)$. Then, we pair a_1 with its modular inverse a_2 as (a_1, a_2). a_1 has 1 modular inverse: a_2 and a_2 has 1 modular inverse: a_1. We can then pair each factor in $2, \cdots, (p-1)$ as: $(a_1, a_2), \cdots, (a_{p-4}, a_{p-3})$. Then,

$$(p-1)! = 1 * (p-1) * (a_1 * a_2) * \cdots * (a_{p-4} * a_{p-3})$$

$$\equiv 1 * (p-1) * 1 * \cdots * 1$$

$$\equiv -1 \pmod{p}$$

(b) (<=) Suppose $(p-1)! \equiv -1 \pmod{p}$. Suppose p is composite. Then it has some prime factor $1 < q < p$. Then q is one of the factors: $1, 2, \ldots, (p-1)$ in $(p-1)!$. Then $(p-1)! \equiv 0 \pmod{q}$.
Since $(p-1)! \equiv -1 \pmod{p}$, we can write $(p-1)!$ as $mp-1$ for some integer m and then write it as $mnq-1$ for some integer n. Then, it follows that $(p-1)! \equiv -1 \pmod{q}$. This is a contradiction, a value can not hold 2 different mod values. Therefore, p must be prime.

4 Celebrate and Remember Textiles

Note 6 You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements on the row lengths of each of the stitch patterns:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: Multiple of 5, plus 2

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

Solution: This is simply the same as finding the smallest positive integer x that satisfies:

$$x \equiv 4 \pmod 7$$

$$x \equiv 2 \pmod 4$$

$$x \equiv 2 \pmod 5$$

Since 7, 4, 5 are all coprime, we can use CRT to solve this:
Let a be a number $\equiv 1 \pmod 7, 0 \pmod 4, 0 \pmod 5$.
Then $(4*5)(-1) \equiv -20 \equiv 1 \pmod 7$ so $a = -20$.
Let b be a number $\equiv 0 \pmod 7, 1 \pmod 4, 0 \pmod 5$.
Then $(7*5)(3) \equiv 105 \equiv 1 \pmod 4$ so $b = 105$.
Let c be a number $\equiv 0 \pmod 7, 0 \pmod 4, 1 \pmod 5$.
Then $(7*4)(2) \equiv 56 \equiv 1 \pmod 5$ so $c = 56$.
Then $x = 4a + 2b + 2c = -80 + 210 + 112 = 242 \equiv 102 \mod 140$. (Where 140 = 7*4*5)
Thus, 102 is the smallest number of stitches you need to cast on in order to incorporate all 3 patterns. We easily verify this by trying 102 on the given equations.

5 Euler's Totient Theorem

Note 6
Note 7

Euler's Totient Theorem states that, if n and a are coprime,

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

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1). Note that this theorem generalizes Fermat's Little Theorem, since if n is prime, then $\phi(n) = n-1$.

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) := ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

Solution:

(a) (1) Lemma: the product of numbers coprime to x is coprime to x. Proof: the numbers do not share any factors with x, so even when they are multiplied together, they still do not share factors with x, thus still coprime.
(2) Lemma: a is coprime to b IFF $a \pmod{b}$ is coprime to b. Proof: we know that a is coprime to b IFF $\gcd(a,b) = 1$. We also know that by Euclid's algorithm: $\gcd(a,b) = gcd(b, a \pmod{b})$. Therefore, it follows that the lemma is correct.
(3) Lemma: $am_1, \ldots, am_{\phi(n)}$ are all distinct $\pmod{n}$. Proof: Suppose $am_i \equiv am_j \pmod{n}$ for some $i > j$. Then $a(m_i - m_j) \equiv 0 \mod n$. Since a is coprime to n, $m_i - m_j$ must be an integer multiple of n. This is impossible, since $m_i - m_j$ is in between 1 and $n-1$. By contradiction, we have proved the lemma.
(4) We know that a and $m_1, \ldots, m_{\phi(n)}$ are all coprime to n. Then, $am_1, \ldots, am_{\phi(n)}$ are all coprime to n. These are all distinct mod n. Then both sets contain all the residues of coprime numbers mod n. Thus we conclude that $am_1, \cdots, am_{\phi(n)}$ is a permutation of $m_1, \cdots, m_{\phi(n)}$.

(b) We have that

$$am_1 * \cdots * am_{\phi(n)} \equiv m_1 * \cdots * m_{\phi(n)} \pmod{n}$$

Then,

$$a^{\phi(n)} * (m_1 * \cdots * m_{\phi(n)}) \equiv (m_1 * \cdots * m_{\phi(n)}) \pmod{n}$$

Since $(m_1 * \cdots * m_{\phi(n)})$ is coprime to n, it has a modular inverse mod n. After multiplying by its modular inverse on both sides, we get that

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

as desired.

6 Sparsity of Primes

Note 6

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find n such that $(n+1)$, $(n+2)$, $\dots$, and $(n+k)$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.

Solution: A number is not a prime power if it has 2 distinct prime divisors. Suppose we have some positive integer k. Let $p_1, \cdots, p_{2k}$ be some list of distinct primes. Now, let n satisfy the following equations:

$$\begin{aligned}
n &\equiv -1 \pmod{p_1} \\
n &\equiv -1 \pmod{p_2} \\
n &\equiv -1 \pmod{p_3} \\
n &\equiv -1 \pmod{p_4} \\
&\vdots \\
n &\equiv -1 \pmod{p_{2k-1}} \\
n &\equiv -1 \pmod{p_{2k}}
\end{aligned}$$

Since all the moduli are primes and are thus coprime with each other, such an n exists due to the Chinese Remainder Theorem.

Then it follows that $n+1, \cdots, n+k$ each have 2 divisors. Thus, for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.