3

Modular Arithmetic

Computer Science Mentors 70

Feb 15 - Feb 19
Spring 2021

Prepared by: Amogh Gupta, Sylvia Jin, Aekus Bhathal, Abinav Routhu, Debayan Bandyopadhyay
Roast us here: *https://tinyurl.com/csm70-feedback20*

1 Modular Arithmetic Properties

We now introduce the concept of *modular arithmetic* (also sometimes known as "clock arithmetic"). Modular arithmetic is a system of algebra in which all mathematical operations are performed relative to a *modulus* or "base".

(Note 6, page 1) We define $x \bmod m$ (in words: "x modulo m") to be the remainder r when we divide x by m.
If $x \bmod m = r$, then $x = mq + r$ where $0 \leq r \leq m - 1$ and q is an integer. Explicitly,

$$x \bmod m = r = x - m\left\lfloor \frac{x}{m} \right\rfloor$$

1. Prove the following: if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ then $a \cdot b \equiv c \cdot d \pmod{m}$. (Theorem 6.1 Note 6)

2. (a) If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ then which of the following are true?
   - $a^b \equiv c^b \pmod{m}$
   - $a^b \equiv a^d \pmod{m}$
   - $a^b \equiv c^d \pmod{m}$

   (b) Prove your answer for part a using the theorem in question 1. If false, also provide a counterexample.

   (c) If $ka \equiv kc \pmod{m}$, does it follow that $a \equiv c \pmod{m}$?

3. Calculate $15^{2021} \pmod{17}$. (Hint: You may want to choose a different representation of 15 in mod 17.)

2 Bijections

(Note 6, Page 4) A *bijection* is a function for which every $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:
1. f is *onto*: every $b \in B$ has a pre-image $a \in A$.
2. f is *one-to-one*: for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$.

Lemma:
For a finite set A, $f : A \longrightarrow A$ is a bijection if there is an *inverse* function $g : A \longrightarrow A$ such that $\forall x \in A \; g(f(x)) = x$.

1. Draw an example of each of the following situations:

One to one AND NOT onto (injective but not surjective)	Onto AND NOT one to one (surjective but not injective)	One to one AND onto (bijection, i.e. injective AND surjective)

2. Define $\mathbb{Z}_n$ to be the set of remainders mod n. In particular, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for any n. Are the following functions **bijections** from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{12}$?

   (a) $f(x) = 7x$

   (b) $f(x) = 3x$

   (c) $f(x) = x - 6$

3. Why can we not have a surjection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{24}$ or an injection from $\mathbb{Z}_{12}$ to $\mathbb{Z}_6$?

4. Prove the following: The function $f(x) = a \cdot x \bmod p$ (where p is prime) is a bijection where $a, x \in \{1, 2, \ldots, p-1\}$.

3 Euclid's Algorithm and Inverses

Euclid's Algorithm: Euclid's algorithm is a method to determine the greatest common factor of two numbers x and y. It hinges crucially on **Note 6, Theorem 6.3** (see question 1).

```
algorithm gcd(x,y)
  if y = 0 then return(x)
  else return(gcd(y,x mod y))
```

Finding Inverses with Euclid's Algorithm: Using Euclid's Algorithm, it is possible to determine the inverse of a number mod n. The inverse of $x \bmod n$ is the number $x^{-1} \equiv y \bmod n$ such that $xy = 1 \bmod n$. The extended algorithm takes as input a pair of natural numbers $x \geq y$ as in Euclid's algorithm, and returns a triple of integers (d, a, b) such that $d = \gcd(x, y)$ and $d = ax + by$:

```
algorithm extended-gcd(x,y)
  if y = 0 then return(x, 1, 0)
  else
    (d, a, b) := extended-gcd(y, x mod y)
    return((d, b, a - (x div y) * b))
```

1. Prove that for $a > b$, if $\gcd(a, b) = d$, then it is also true that $\gcd(b, a \bmod b) = d$. (Theorem 6.3 Note 6)

2. (a) Run Euclid's algorithm to determine the greatest common divisor of $x = 6$, $y = 32$.

   (b) Run Euclid's algorithm to determine the greatest common divisor of $x = 13$, $y = 21$. (Practice Bank, Set 4, 4c)

   (c) Use the Extended Euclid's Algorithm to find the two numbers a, b such that $13a + 21b = 1$.

(d) Given your answers to the previous parts, is there a multiplicative inverse for $13 \mod 21$? If so, what is it? Similarly, what is the inverse of $21 \mod 13$?

3. The last digit of $8k + 3$ and $5k + 9$ are the same for some k. Find the last digit of k.

4 Advanced Leapfrog

4. Suppose we have 7 vertices, each of which corresponds to a different integer modulo seven. Draw an (undirected) edge between two vertices x and y if $x + 3 \equiv y \mod 7$. For example, there is an edge between 0 and 3, and an edge between 5 and 2. What is the length of the shortest path between 0 and 1?

5. Suppose we have a similar setup to part 1, except now we have p vertices, for prime p, each of which corresponds to a different integer mod modulo p. Draw an edge between x and y if $x + c \equiv y \mod p$. What are the possible candidates for the length of the shortest path between 0 and 1? (As this depends on the constant c and the modulus p, the answer should be in terms of modular equivalences.)

5 CRT

1. Suppose we have a number v, which we do not know, but which satisfies the following system of modular equivalences. The numbers n, l, and m are coprime to each other.

$$v \equiv a \mod \ell$$
$$v \equiv b \mod m$$
$$v \equiv c \mod n$$

We want to use the numbers a, b, and c, which we do know, to reconstruct v.

Just for this worksheet, we will compactly write the system of modular equivalences as a tuple, for example, $v \equiv (a, b, c)$.

(a) Construct a number x' which is zero mod m and mod n, but is nonzero mod ℓ.

(b) Using x' from the previous part, construct a number x which is still zero mod m and mod n, but is now 1 mod ℓ. In other words, find $x \equiv (1, 0, 0)$.

(c) We want to do the same with the other two moduli. Find $y \equiv (0, 1, 0)$ and $z \equiv (0, 0, 1)$.

(d) Using the numbers x, y, z above, construct numbers $x'' \equiv (a, 0, 0)$, $y'' \equiv (0, b, 0)$, $z'' \equiv (0, 0, c)$.

(e) Using the numbers x, y, and z above, construct a number v which satisfies our system of modular equivalences. Is this the only number v that satisfies this system of equivalences? Why or why not?

(f) If two numbers v and w both satisfy the system of modular equivalences, meaning $v \equiv (a, b, c) \equiv w$, show that $v \equiv w \mod \ell mn$.

2. The supermarket has a lot of eggs, but the manager is not sure exactly how many he has. When he splits the eggs into groups of 5, there are exactly 3 left. When he splits the eggs into groups of 11, there are 6 left. What is the minimum number of eggs at the supermarket?

3. Your best friend's birthday is in roughly 2 months but you don't remember the exact date, so you plan to ask the Greek Gods for help. After praying a lot, Zeus, Hades and Poseidon appear in front of you, say these sentences and leave.

   Zeus: If you count days 3 at a time, you will miss your friend's birthday by 2 days.

   Hades: If you count days 4 at a time, you will miss your friend's birthday by 3 days.

   Poseidon: If you count days 5 at a time, you will miss your friend's birthday by 4 days.

   Find your friend's birthday if today is December 1^{st}.