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 $0 \le r \le m - 1$ 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)

Solution: Let $a = c + km$ and $b = d + lm$ for integers k, l. Then $a \cdot b \equiv (c+km)(d+lm) \equiv cd + dkm + clm + klm^2 \equiv c \cdot d \pmod m$.

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

   - $a^b \equiv c^b \pmod m$
   - $a^b \equiv a^d \pmod m$
   - $a^b \equiv c^d \pmod m$

   Solution: Only the first one is true.

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

   Solution:

   - We have b copies of a repeatedly multiplied by each other. We could repeatedly use the theorem from question 1 to replace each of these with c in the multiplication and it would be equivalent. This could be proved more rigorously using induction.
   - Here is a counterexample: $2^5 \equiv 2 \not\equiv 1 \equiv 2^2 \pmod 3$
   - Here is a counterexample: $2^2 \equiv 1 \not\equiv 2 \equiv -1 \equiv (-1)^5 \pmod 3$

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

   Solution: No. Here is a counterexample: $10 \equiv 6 \pmod 4$, but $5 \not\equiv 3 \pmod 4$.

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

Solution: Instead of using brute repeated exponentiation, we can convert this to a more manageable form: $(-2)^{2021} \pmod{17}$ since $15 \equiv -2 \pmod{17}$. Now we notice that $(-2)^4 \equiv 16 \equiv -1 \pmod{17}$. Hence,

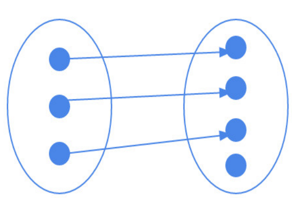
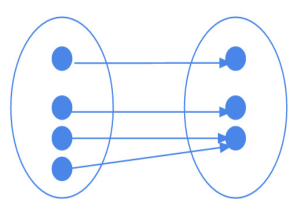
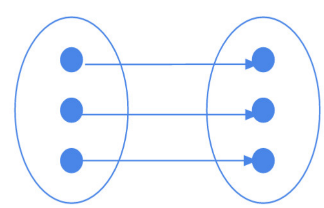
$$\begin{aligned}
15^{2021} &\equiv (-2)^{2021} && \pmod{17} \\
&\equiv ((-2)^4)^{505} \cdot -2 && \pmod{17} \\
&\equiv (-1)^{505} \cdot -2 && \pmod{17} \\
&\equiv -1 \cdot -2 && \pmod{17} \\
&\equiv 2 && \pmod{17}
\end{aligned}$$

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)
Solution: . 	**Solution:** . 	**Solution:** . 

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) $f(x) = 7x$

   Solution: Yes: the mapping works. Since 7 is coprime to 12, there exists a multiplicative inverse to 7 in $\mathbb{Z}_{12}$ ($7 \times 7 = 49 \bmod 12 = 1$, so $f^{-1}(x) = 7x$), which only occurs if the function is a bijection.

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

   Solution: No. For example, $f(0) = f(4) = 0$.

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

Solution: Yes. It's just $f(x) = x$, shifted by 6. Note: we can write an explicit inverse $f^{-1}(x) = x + 6$, which means a bijection exists.

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

Solution: Because there are more values in $\mathbb{Z}_{24}$ than $\mathbb{Z}_{12}$, it is impossible to cover all the values in $\mathbb{Z}_{24}$ by mapping from $\mathbb{Z}_{12}$. Similarly, because there are more values in $\mathbb{Z}_{12}$ than $\mathbb{Z}_6$, there are not enough unique elements in $\mathbb{Z}_6$ to assign one to every element in $\mathbb{Z}_{12}$. In general, for finite sets A, B, a mapping $A \longrightarrow B$ is a surjection only if A is at least as big as B ($|A| \geq |B|$), and it's an injection only if $|B| \geq |A|$. Note that these are **necessary** but not sufficient conditions.

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

Solution: The domain and range of the function are the same set (and thus have the same cardinality), so it is enough to show that if $x \neq x'$ then $a \cdot x \bmod p \neq a \cdot x' \bmod p$ (injectivity).
Assume that $a \cdot x \bmod p \equiv a \cdot x' \bmod p$ for $x \not\equiv x' \bmod p$.
Since $\gcd(a, p) = 1$, a must have an inverse $a^{-1} \bmod p$:

$$ax \bmod p \equiv ax' \bmod p$$

$$a^{-1} \cdot a \cdot x \bmod p \equiv a^{-1} \cdot a \cdot x' \bmod p$$

$$x \bmod p \equiv x' \bmod p$$

This contradicts our assumption that $x \neq x' \bmod p$. Therefore f is a bijection. □

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)

Solution: The theorem follows from the fact that a number d is a common divisor of a and b if and only if d is a common divisor of a and $(a \bmod b)$. To see this, write $a = qb + r$ where q is an integer and $r = a \bmod b$. Then, if d divides a and b then it also divides a and qb, and thus it also divides their difference $r = a - qb$ (as we proved in Theorem 6.1). Conversely, if d divides b and r then it also divides qb and r and thus also their sum $a = qb + r$.

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

Solution: Running Euclid's algorithm, $\gcd(32, 6) = \gcd(6, 2) = \gcd(0, 2) = 2$. By the Extended Euclid's algorithm, we can also find what coefficients satisfy $6a + 32b = 2$:

$$\begin{aligned} 2 &= 6 - 2(2) \\ &= 6 - (32 - 5(6))(2) = 6(11) - 32(2) \end{aligned}$$

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

Solution: Euclid's algorithm says when $a > b$, $\gcd(a, b) = \gcd(b, a \bmod b)$. Thus, $\gcd(21, 13) = \gcd(13, 8) = \gcd(8, 5) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0) = 1$.

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

Solution: Using Inverse Euclid's algorithm which uses back-substitution, we have a way to systematically find m and n that satisfy the equation: $\gcd(m, n) = d = am + bn$ for some natural numbers a and b.

$\gcd(21, 13)$	21 = 13(1) + 8	8 = 21 - 13(1)	(5)
$\gcd(13, 8)$	13 = 8(1) + 5	5 = 13 - 8(1)	(4)
$\gcd(8, 5)$	8 = 5(1) + 3	3 = 8 - 5(1)	(3)
$\gcd(5, 3)$	5 = 3(1) + 2	2 = 5 - 3(1)	(2)
$\gcd(3, 2)$	3 = 2(1) + 1	1 = 3 - 2(1)	(1)
$\gcd(2, 1)$			
$\gcd(1, 0)$			

$$\begin{aligned} 1 &= 3 - 2(1) && (1) \\ &= 3 - (5 - 3(1))(1) = 3(2) - 5(1) && (2) \\ &= (8 - 5(1))(2) - 5(1) = 8(2) - 5(3) && (3) \\ &= 8(2) - (13 - 8(1))(3) = 8(5) - 13(3) && (4) \\ &= (21 - 13(1))(5) - 13(3) = 21(5) - 13(8) && (5) \end{aligned}$$

You may notice that this equation took many more steps than the previous part, but the overall algorithm has a runtime of $O(\ln n)$, where n is the bigger number. In fact, the numbers that take the longest time to finish are the *Fibonacci numbers*, a sequence defined by $f_0 = 0, f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ (in fact, $f_7 = 13, f_8 = 21$). Roughly, it's because each step can only take away 1 multiple of the smaller number.

(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?

Solution: From the previous part, we have $1 = 21(5) - 13(8)$. The inverse of a number n is the number m such that $nm \equiv 1$.

To find the inverse of 13 mod 21, take mod 21 on both sides of the equation. Then, we have $1 \equiv 13(-8) \equiv 13(13) \mod 21$, so the inverse of 13 is 13.

Similarly, to find the inverse of 21 mod 13, take mod 13 on both sides of the equation. Then, we have $1 \equiv 21(5)$, so the inverse of 21 is 5.

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

Solution: We can get the last digit of the numbers by taking them each $\bmod 10$. Now we have $8k+3 \equiv 5k+9 \pmod{10}$ since their last digits are the same. Solving for k's last digit,

$$\begin{aligned} 8k + 3 &\equiv 5k + 9 && \pmod{10} \\ 8k - 5k &\equiv 9 - 3 && \pmod{10} \\ 3k &\equiv 6 && \pmod{10} \\ k &\equiv 6 \cdot 3^{-1} && \pmod{10} \\ k &\equiv 6 \cdot 7 && \pmod{10} \\ k &\equiv 2 && \pmod{10} \end{aligned}$$

So the last digit of k is 2.

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 $x + 3 \equiv y \bmod 7$. 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?

Solution: Suppose we travel from 0 along the edges that correspond to adding 3. The length of this path will be the n that satisfies $3n \equiv 1 \bmod 7$. Instead, suppose we travel from 1 along the edges that correspond to adding 3. Then, the length of the path will be m such that $1 + 3m \equiv 0 \bmod 7$. The multiplicative inverse of 3 modulo 7 is 5. Thus, $n = 5$ and $m = 2$, so the shortest path is length 2.

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 $x + c \equiv y \bmod p$. 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.)

Solution: Using a similar reasoning, the two candidates are n such that $cn \equiv 1 \bmod p$ and m such that $1+cm \equiv 0 \bmod p$. We can succinctly write the solution as $\min\{c^{-1} \bmod p,\ (p-1)c^{-1} \bmod p\}$.

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.

$$\begin{aligned} v &\equiv a \mod \ell \\ v &\equiv b \mod m \\ v &\equiv c \mod n \end{aligned}$$

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.

Solution: A number which is zero mod m and mod n must be a multiple of m and n. We can choose $x' = mn$. Because m and n share no factors with ℓ, $x' = mn$ is not a multiple of ℓ, so it 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 $x \equiv (1, 0, 0)$.

> **Solution:** Because m and n are coprime to ℓ, $x' = mn$ has a multiplicative inverse mod ℓ. If we multiply x' by the inverse of mn, we can scale x' to be 1 mod ℓ. In symbols, $x = ((mn)^{-1} \bmod \ell)x' \equiv 1 \bmod \ell$. Because it is still a multiple of m and of n, it will still be zero in those moduli.

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

> **Solution:** Following the same process, $y = \ell n((\ell n)^{-1} \bmod m)$, and $z = \ell m((\ell m)^{-1} \bmod n)$.

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

> **Solution:** Consider $x'' = ax, y'' = by, z'' = cz$. Without loss of generality, $x' \equiv (a, 0, 0)$ because $ax = a(1, 0, 0) = (1a, 0a, 0a) \equiv (a, 0, 0)$. Using the same logic, y'' and z'' also satisfy their respective congruences.

(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?

> **Solution:** Consider $v = x'' + y'' + z''$ (which also equals $ax + by + cz$). We've scaled up the relevant bit in each modulus and added them together. The amount that we scale x by has no effect on the equivalence mod m and mod n, since $c0 = 0$ for any c, but allows us to match the condition $v \equiv a \bmod \ell$. This is not the only solution, as we can add multiples of ℓmn to our solution and still satisfy the above equivalences.

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

> **Solution:** Consider the number $v - w$. Because v and w are the same under the three different modular equivalences, subtracting them will just give zero under each modulus. Now we use the procedure above to reconstruct $v - w = (0, 0, 0)$. This gives $v - w = 0x + 0y + 0z = 0$. So $v - w = 0$ is a valid solution to this system of equivalences, but from our previous answer, we know that any multiple of ℓmn can be added to this. Thus, $v - w \equiv 0 \bmod \ell mn$, which implies that $v \equiv w \bmod \ell mn$.

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?

> **Solution:** We have that $x \equiv 3 \bmod 5$ and $x \equiv 6 \bmod 11$. We can use the Chinese Remainder Theorem to solve for x.
>
> Recall from the note on modular arithmetic, the solution to x is defined as $x = \left(\sum_{i=1}^{k} a_i b_i\right) \bmod N$, where b_i are defined as $\left(\frac{N}{n_i}\right)\left(\left(\frac{N}{n_i}\right)^{-1} \bmod n_i\right)$ and $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ is the product of the moduli.
>
> In our case, $a_1 = 3$, $a_2 = 6$, $n_1 = 5$ and $n_2 = 11$. First find the b_i:
>
> $$b_1 = \left(\frac{55}{5}\right)\left(\left(\frac{55}{5}\right)^{-1} \bmod 5\right) = 11 \cdot \left(11^{-1} \bmod 5\right) = 11 \cdot 1 = 11$$

$$b_2 = \left(\frac{55}{11}\right)\left(\left(\frac{55}{11}\right)^{-1} \bmod 11\right) = 5 \cdot \left(5^{-1} \bmod 11\right) = 5 \cdot 9 = 45$$

Therefore, $x \equiv a_1 b_1 + a_2 b_2 \equiv 3 \cdot 11 + 6 \cdot 45 \pmod{55} \equiv 28 \pmod{55}$.

You can quickly verify that 28 indeed satisfies both conditions.

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}.

Solution: We can setup 3 equations by the three sentences of the Greek Gods.

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

Let us solve the system of equations using CRT:
we have $a_1 = 2, a_2 = 3, a_3 = 4$ and $n_1 = 3, n_2 = 4, n_1 = 5$ so $N = \prod_{i=1}^{3} n_i = 3 \cdot 4 \cdot 5 = 60$
We now calculate b_i. First we calculate the three $\frac{N}{n_i}$:

$$N_1 = \frac{N}{3} = 20, \quad N_2 = \frac{N}{4} = 15, \quad N_3 = \frac{N}{5} = 12$$

Second we calculate multiplicative inverses $\pmod{n_i}$ of $\frac{N}{n_i}$

$$\begin{aligned} m_1 &= (N_1)_{n_1}^{-1} = 20_3^{-1} = 2 \quad (\text{Notice} \quad 20 \cdot 2 = 40 \equiv 1 \pmod{3}) \\ m_2 &= (N_1)_{n_1}^{-1} = 15_4^{-1} = 3 \quad (\text{Notice} \quad 15 \cdot 3 = 45 \equiv 1 \pmod{4}) \\ m_3 &= (N_1)_{n_1}^{-1} = 12_5^{-1} = 3 \quad (\text{Notice} \quad 12 \cdot 3 = 36 \equiv 1 \pmod{5}) \end{aligned}$$

Finally we have $x = \sum_{i=1}^{3} a_i m_i N_i = 2 \cdot 2 \cdot 20 + 3 \cdot 3 \cdot 15 + 4 \cdot 3 \cdot 2 = 20 + 15 + 24 = 59 \pmod{60}$

Alternate solution: But there is a simpler way to solve this. We notice that $2 \equiv -1 \pmod{3}, 3 \equiv -1 \pmod{4}, 4 \equiv -1 \pmod{5}$:

$$\begin{aligned} x &\equiv -1 \pmod{3} \\ x &\equiv -1 \pmod{4} \\ x &\equiv -1 \pmod{5} \end{aligned}$$

Then $x = -1$ is a solution for the system of equations. Now by CRT $x \equiv -1 \equiv 59 \pmod{60}$.

That means your friend's birthday is after 59 days from today, which puts it on 29^{th} January.