Week 6 Introductory: Modular Arithmetic I

Math Divulged

June 15, 2020

§1 Introduction

Definition 1.1. We define a, b **congruent modulo** n:

$$a \equiv b \pmod{n}$$

if and only if $n \mid a - b$. This can also be interpreted as a and b sharing the same remainder upon division by n.

Example 1.2

What numbers n satisfy $n \equiv 3 \pmod{5}$?

Solution. By the definition of the congruence, $n - 3$ is an integer multiple of 5. In mathematical terms, we can write $n - 3 = 5k$ where k is an integer. Solving this, we get that n can be any number of the form $5k + 3$ where k is any integer, positive or negative. □

It's important to observe that the numbers used in congruences can also be negative. For instance, $7 \equiv -1 \pmod{8}$. Congruences also differ between different mods, so don't expect one congruence in one mod to necessarily hold under the modulo of another number.

§1.1 Properties

The "three-lines equal sign" symbol used for congruences works remarkably similar to the ordinary equal sign. In fact, the following properties are true:

Theorem 1.3

(i) Reflexivity: $a \equiv a \pmod{n}$.
(ii) Symmetry: If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
(iii) Transitivity: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(iv) If $a \equiv b \pmod{n}$ and if $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$. The same goes for subtraction.
(v) Associativity, Commutativity, and Distribution/Factoring holds.
(vi) If $a \equiv b \pmod{n}$ and if $c \equiv d \pmod{n}$, then $a \cdot c \equiv b \cdot d \pmod{n}$.
(vii) If $a \equiv b \pmod{n}$, then for an integer k, $a^k \equiv b^k \pmod{n}$.

It's relatively easy to prove all of these using the definition of a congruence. However, understanding how to use these principles is much more useful, as these build the foundation for why modular arithmetic can be so powerful.

Example 1.4

Find the remainder of $236 \cdot 237 + 961$ when it is divided by 8.

Solution. Instead of directly evaluating the large number and then dividing by 8, we can use the properties of modular congruences listed in Theorem 1.3.

Using property (vi), we can observe that we can find congruent mods for 236 and 237 each, and simply multiply those. This is much easier, as $236 \equiv 4 \pmod 8$ and $237 \equiv 5 \pmod 8$. So,

$$236 \cdot 237 \equiv 4 \cdot 5 \pmod 8.$$

Next, instead of adding to 961, we can first evaluate $961 \equiv 1 \pmod 8$. So, through property (iv),

$$236 \cdot 237 + 961 \equiv 4 \cdot 5 + 1 \equiv \boxed{5} \pmod 8.$$

□

Example 1.5

Find the remainder of 36^{2020} when it is divided by 37.

Solution. In this problem, computing the expression isn't even an option. However, property (vii) of Theorem 1.3 makes quick work of this if we pick the right congruences to work with. Notice that $36 \equiv -1 \pmod{37}$. Using the property, we know that

$$36^{2020} \equiv (-1)^{2020} \equiv \boxed{1} \pmod{37}$$

is our answer. □

We can add, subtract, and multiple congruent relations to both sides of a congruence. Just these properties we have used alone can help simplify many seemingly impossibly questions.

However, division is not allowed. For instance, $16 \equiv 6 \pmod{10}$ but dividing by 2 fails because $8 \equiv 3 \pmod{10}$ is not true. But this is something mathematicians can combat.

§2 Solving Linear Congruences

Example 2.1

Will has thought of a number x between 15 and 30. He puts it into his number machine, which multiplies a number by 4 and then adds 7 to it. After receiving this new number, Will laughs and says that when he divides the new number by 15, the remainder is 3. Find x.

Solution. Since the problem revolves around divisibility and remainders, we should immediately write it in terms of modular arithmetic. The number machine produces the expression $4x + 7$ which we are told satisfies $4x + 7 \equiv 3 \pmod{15}$. We can subtract 7 from both sides of the congruences, so $4x \equiv -4 \equiv 11 \pmod{15}$. But how do we get rid of the 4? Division does not work in modular arithmetic like we mentioned earlier. However, notice what happens when we multiply both sides by 4:

$$4x \cdot 4 \equiv 11 \cdot 4 \pmod{15} \implies 16x \equiv x \equiv 44 \equiv 14 \pmod{15}.$$

Since we are told that x was between 15 and 30, the only number there with a remainder of 14 when divided by 15 is $\boxed{29}$. □

The clever trick we pulled to get rid of the coefficient of 4 on x in that problem was to realize that multiplying 4 again would reduce the coefficient to 1 (using Theorem 1.3). This would directly give us what x was congruent to.
This trick wasn't a coincidence, but rather a real concept.

§2.1 Defining Inverses

Definition 2.2. The number b is called a multiplicative inverse of a modulo n if

$$ab \equiv 1 \pmod{n}.$$

We usually write $a^{-1} = b$.

In terms of modular arithmetic, this is the analogy to division we see in ordinary numbers. For instance, dividing 3 by 3 to get 1 is really just multiply 3 by 1/3, and we call 1/3 the multiplicative inverse. Thus, fractions like 2/3 are just 2 multiplied by the inverse of 3.

In example 2.1, we realized that $4^{-1} \equiv 4 \pmod{15}$ because $4 \cdot 4 \equiv 1 \pmod{15}$. Thus, we multiplied both sides of the equation by the inverse to convert $4x$ into just x.

However, some numbers will not have inverses. For instance, you can try, but there is no number x such that $3x \equiv 1 \pmod{15}$. So, when do we know an inverse exists?

Theorem 2.3

For an integer a, there exists an integer a^{-1} such that

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

if and only if a and n are relatively prime, that is, $\gcd(a, n) = 1$.

The proof of this theorem uses Bezout's identity.

Usually, especially for smaller numbers, it's easy to quickly guess what the inverse is. However, sometimes the numbers are too large. In this case, there is a technique known as the **Extended Euclidean Algorithm** to compute the inverse. I'll demonstrate it in class, but I'm sure you can google this as well.

§2.2 Multiple Congruences

Problems won't always require solving one congruence. In some instances, there will be multiple congruences of different modulo.

Theorem 2.4 (Chinese Remainder Theorem)

If $m_1, \ldots, m_n$ are pairwise relatively prime, then the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

has a solution modulo $m_1 m_2 \cdot \ldots \cdot m_n$.

This theorem, commonly abbreviated CRT, only tells us that a solution can exist. However, there is a straightforward method to actually solve a system.

Example 2.5

Solve the congruences:

$$x \equiv 2 \pmod 5$$
$$x \equiv 1 \pmod 7.$$

Solution. By CRT, we should be aware that we are looking for an answer $x \pmod{35}$. However, let's look at the first congruence. Using the definition of a congruence, this can be written as $x = 5a + 2$ for an integer a. Substituting this into the second congruence gives

$$5a + 2 \equiv 1 \pmod 7 \implies 5a \equiv 6 \pmod 7.$$

We can solve this congruence by noticing that $5^{-1} \equiv 3 \pmod 7$ and so

$$5a \cdot 3 \equiv a \equiv 6 \cdot 3 \equiv 4 \pmod 7.$$

Using the definition of a congruence again, we can write $a = 7b + 4$ for some integer b. Substituting this back into our equation for x gives

$$x = 5a + 2 = 5(7b + 4) = 35b + 22 \implies \boxed{x \equiv 22 \pmod{35}}.$$

□

Though we did this process for two congruences, this can easily be repeated over and over for many congruences. If a problem asks to find a number given multiple remainders for multiple divisors, this approach will allow you to solve it effectively.

§3 Cycles

In this section, we will primarily cover the topic of exponents in modular arithmetic. Exponents will always cycle back to themselves.

Example 3.1

Find the last digit of 2^{2020}.

Solution. The last digit is simply the remainder when divided by 10, so we are searching for $2^{2020} \pmod{10}$. If we evaluate powers of 2 modulo 10, we have 2, 4, 8, 6, and then 2 again. And if we keep going, this just loops through these numbers over and over. Thus, a cycle is occuring, and the cycle repeats every 4 numbers. In other words, $2^4 \equiv 6 \pmod{10}$ and $2^8 \equiv 6 \pmod{10}$ and any $2^{4k} \equiv 6 \pmod{10}$ for integer $k > 0$. Since 2020 is a multiple of 4, we know that $2^{2020} \equiv \boxed{6} \pmod{10}$. □

The cycle length for 2 won't always be 4 for each mod. It will vary for every number. As you can imagine, it can be frustratingly difficult to look for cycles for larger numbers and larger modulo. How can we reduce the effort we need to evaluate exponents in modular arithmetic?

§3.1 Totient

There is a tool we can use, but we need to introduce a new function first.

Definition 3.2. The totient function $\phi(n)$ is equal to the number of integers less than n that are relatively prime to n.

It turns out, through some simple counting tricks, that there is an explicit formula for the totient function.

Theorem 3.3

For an integer $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ where $p_1, ..., p_m$ are unique primes in its factorization,

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

As an example,

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$$

§3.2 Euler's Theorem

Theorem 3.4

Given two relatively prime integers a and n,

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

The significance in this theorem is that it immediately reveals a cycle. Although this cannot be used on example 3.1 since $\gcd(2, 10) \neq 1$, it can be applied most of the time for larger numbers where computation is brutal.

Example 3.5

Find the last two digits of 17^{122}.

Solution. Last two digits implies we are looking in modulo 100. Since $\phi(100) = 40$, $17^{40} \equiv 1 \pmod{100}$. Using this cycle, we can write

$$17^{122} = (17^{40})^3 \cdot 17^2 \equiv 17^2 \equiv \boxed{89} \pmod{100}.$$

□

These type of problems show up relatively frequently on a variety of competitions, and knowing Euler's theorem is a huge advantage when it comes to speed. Most cycles should and can be simplified greatly with Euler's, and the remaining computation should be done by hand. It is worth noting that the easiest way to compute powers by hand is by squaring repeatedly and using binary to build up to a particular exponent.

In conclusion, modular arithmetic is a powerful tool for to simplify various problems. However, make sure you keep your eyes open to patterns before fully relying on theorems and various tricks.

§4 Problems

Problem 4.1. Prove that for any integer n, the sum of its digits S satisfies $S \equiv n \pmod 9$.

Problem 4.2 (1999 AMC 8)**.** What is the remainder when 1999^{2000} is divided by 5?

Problem 4.3 (2010 AIME)**.** Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots 9}_{\text{999 9's}}$ is divided by 1000.

Problem 4.4 (AMC 12)**.** Mrs. Walter gave an exam in a mathematics class of five students. She entered the scores in random order into a spreadsheet, which recalculated the class average after each score was entered. Mrs. Walter noticed that after each score was entered, the average was always an integer. The scores (listed in ascending order) were 71, 76, 80, 82, and 91. What was the last score Mrs. Walters entered?

Problem 4.5 (2009 AMC 10)**.** What is the remainder when $3^0 + 3^1 + 3^2 + \cdots + 3^{2009}$ is divided by 8?

Problem 4.6. Helen is thinking of a number n. When divided by 9, it has a remainder of 2. When divided by 11, it has a remainder of 8. When divided by 5, it has a remainder of 3. Given that Helen can only count up to 1000, find the sum of all possible n.

Problem 4.7 (2010 AMC 10)**.** The number obtained from the last two nonzero digits of 90! is equal to n. What is n?