An Introduction to Modular Arithmetic

Sunay Joshi
BCA Math Team AMC Lecture

September 28, 2019

§1 Introduction: clock arithmetic

Modular arithmetic is often introduced by discussing "clock arithmetic". As we all know, an analog clock has an hour hand that travels around from 12 o'clock (midnight) until it hits 12 o'clock (noon), repeating the following cycle of numbers: $12, 1, 2, 3, \dots, 11, 12, 1, 2, \dots$.

Let's say the time is 1 o'clock. After 5 hours, the time will be $1 + 5 = 6$ o'clock. Now say the time is 9 o'clock. In this case, what will be the time after 5 hours? If we add naively, we get $9 + 5 = 14$ o'clock, which doesn't make sense. The correct answer is 2 o'clock, since our cycle repeats every 12 hours. In other words, when we calculate $9 + 5 = 14$, we need to subtract 12 from this value, essentially finding the remainder upon division by 12.

For our purposes, we'll replace 12 with 0. Our observation in the above discussion tells us that when we work with clocks, all times (in hours) are replaced with the remainder they leave when divided by 12. In this "clock arithmetic" system, it makes sense to say that "$9 + 5 = 2$": as $9 + 5$ and 2 share the same remainder when divided by 12, they are equivalent times from the clock's perspective. In the same way, we can say that "$27 = 15 = 3$", as they all leave the same remainder when divided by 12.

In general, given any two numbers, we can formulate the following notion that indicates equivalence if their remainders are the same.

Definition 1.1 (Congruence)**.** We say a **is congruent to** b **modulo** n if a and b leave the same remainder when divided by n. If a is congruent to b modulo n, we write $a \equiv b \pmod{n}$.

Although the above definition may seem daunting, don't worry: it's all about remainders! When we write "$a \equiv b \pmod{n}$", we are simply indicating that a and b are "equal" in the sense that they have the same remainder when divided by n. They are "equivalent" in the sense that, for the most part, they can are interchangeable when finding the remainder a complex expression leaves when divided by n.

Think back to clock arithmetic: we said "$27 = 15 = 3$" on a clock. We were essentially stating that $27 \equiv 15 \equiv 3 \pmod{12}$: that all three leave the same remainder (of 3) when divided by 12.

Remainder calculations are often phrased as "find $a \pmod{n}$". Using "modular equations" as described above allows us to find the remainder a leaves when divided by n through a number of steps. The remainder a leaves when divided by n is sometimes called the **residue** of $a \pmod{n}$. The set of all integers that leave the same residue $r \pmod{n}$ is called the **residue class** of r.

§2 Basic arithmetic

Three basic modular arithmetic calculation tricks:

1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$. In simple terms, "you can substitute in residues while adding $\pmod{n}$". (The same goes for subtraction.)

   As an example, say we wanted to find the remainder when $2019 + 1729$ is divided by 11. We *could* sum $2019 + 1729 = 3748$ and then find its remainder when divided by 11, but that would take a while. To do this with Trick #1, we replace 2019 with its residue of $6 \pmod{11}$ and we replace 1729 with its residue of $2 \pmod{11}$. Our answer is simply $6 + 2 \equiv 8 \pmod{11}$, i.e. a remainder of 8.

2. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \cdot c \equiv b \cdot d \pmod{n}$. In simple terms, "you can substitute in residues while multiplying $\pmod{n}$".

   As an example, say we wanted to find the remainder when $2019 \cdot 1729$ is divided by 11. Multiplying this out would take forever! Instead, since $2019 \equiv 6 \pmod{11}$ and $1729 \equiv 2 \pmod{11}$, the answer is simply $6 \cdot 2 = 12 \equiv 1 \pmod{11}$, i.e. a remainder of 1.

   Very important warning: division *does not work* normally in modular arithmetic! We won't cover it here, but see the "Further reading" section for info.

3. If $a \equiv b \pmod{n}$ and if m is a positive integer, then $a^m \equiv b^m \pmod{n}$. In simple terms "you can substitute in the residue of the **base** of an exponent $\pmod{n}$".

   The reason why this works comes from our multiplication rule. Let's try to prove Trick #3 for an exponent of $m = 4$. The exponential a^4 can be written as $a \cdot a \cdot a \cdot a$. Since each of these factors is congruent to $b \pmod{n}$, this product is congruent to $b \cdot b \cdot b \cdot b = b^4 \pmod{n}$.

   As an example, let's try a problem that would be impossible via brute force: find the remainder when 2015^{2015} is divided by 2014. This is trivial with our formula! As $2015 \equiv 1 \pmod{2014}$, $2015^{2015} \equiv 1^{2015} = 1 \pmod{2015}$, i.e. the remainder is 1.

   Another very important warning: note that you **cannot** substitute in residues for the exponent m! For example, consider $2^{10} \pmod{3}$. The correct answer is $(-1)^{10} \equiv 1 \pmod{3}$ (as $2 \equiv -1 \pmod{3}$). However, if we replace the exponent 10 with its residue $1 \pmod{3}$, we get the *incorrect* answer of $2^1 = 2$. Thus, always keep in mind that **the modulus applies only to the base!**

As you can tell, finding remainders with modular arithmetic is fast! Try the following problems by yourself.

Problem 2.1. Find the remainder when 555^2 is divided by 13.

Problem 2.2. Is $21^{100} - 12^{100}$ a multiple of 11? (*Hint:* use Trick #3 along with the idea of "negative bases" shown above.)

Modular arithmetic is used in a variety of contexts. Aside from computing remainders, it can also provide information about the last digits of a number. In general, the last k digits of a number N is simply the residue N leaves $\pmod{10^k}$. (For instance, the last two digits of N is the residue of $N \pmod{100}$.)

§3 Exponential tricks

Throughout this section, we'll be dealing with the basic question of how to compute $a^b \pmod{n}$. (We use this notation throughout the section.)

§3.1 Pattern finding / inspection of small powers

The technique of pattern finding involves inspecting the residues of small powers of a taken $\pmod{n}$. It's best illustrated by example. Consider the following problem: "What is the remainder when 3^{2019} is divided by 5?" To solve this problem, we start listing out the residues of small powers of 3, starting with 3^0: $3^0 \equiv 1 \pmod{5}$, $3^1 \equiv 3 \pmod{5}$, $3^2 \equiv 4 \pmod{5}$, $3^3 \equiv 2 \pmod{5}$, $3^4 \equiv 1 \pmod{5}$, $3^5 \equiv 3 \pmod{5}$... Once we hit 3^4, we notice that the residues cycle in groups of 4: $1, 3, 4, 2, 1, 3, 4 \ldots$. We notice that only the remainder the exponent leaves when divided by 4 matters: given an exponential 3^m, we can compute $3^m \pmod{5}$ by reducing $m \pmod{4}$. As $2019 \equiv 3 \pmod{4}$, the answer is $3^3 = 27 \equiv 2 \pmod{5}$, i.e. a remainder of 2.

Try using pattern finding / inspection of small powers to solve the following problem.

Problem 3.1. What is the remainder when 7^{2015} is divided by 48?

§3.2 Negative bases

Trick #3 tells us to replace a with its residue $\pmod{n}$. However, sometimes the residue of $a \pmod{n}$ is pretty large. Take, for instance, the case when $a = 2000$, $b = 10$, and $n = 2001$. The remainder when 2000 is divided by 2001 is just 2000, which isn't of much help in our situation. However, if we simply subtract an *extra* $n = 2001$ from a to find the equivalent residue of $2000 - 2001 \equiv -1 \pmod{2001}$, the calculation becomes trivial: it's simply $(-1)^{10} = 1 \pmod{2001}$. Using negative bases can be of great help in reducing the magnitude of the base of the exponential.

Try using negative bases to solve the following problem. Also, try Problem 2.2 if you haven't solved it yet.

Problem 3.2. Find the remainder when $5^{4^{3^{2^{1}}}}$ is divided by 6.

§3.3 Binomial Theorem

Although pattern finding is a powerful technique, it has its limitations. Sometimes, the cycle of exponents is *very long,* making pattern finding infeasible. In such cases, an alternative is to use a clever application of the **Binomial Theorem**. As a reminder, the Binomial Theorem states that for any $x, y \in \mathbb{R}$ and for any positive integer n,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} = x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \ldots + x^0 y^n.$$

In finding $a^b \pmod{n}$, we can sometimes use the Binomial Theorem by breaking up $a = c + d$, where c shares many factors with n. When we expand $(c+d)^n$, we want many of the powers of c to vanish $\pmod{n}$, yielding a simple expression.

Consider the following example: "What are the last two digits of 11^{99}?" In order to find $11^{99} \pmod{100}$, we write $11 = 10 + 1$ and use the Binomial Theorem to write

$$(10+1)^{99} = 10^0 + \binom{99}{1} 10^1 + \binom{99}{2} 10^2 + \ldots + \binom{99}{99} 10^{99}.$$

This is where the idea of choosing c having many common factors with n comes into play: since $10^2 = 100 \equiv 0 \pmod{100}$, all terms after the second vanish $\pmod{100}$! Thus, the final answer is $10^0 + \binom{99}{1}10^1 = 1 + 990 = 991 \equiv 91 \pmod{100}$, i.e. the last two digits of 91.

As you can see from the above example, choosing c such that c^t is divisible by n can be *especially* useful when using the Binomial Theorem. Try the following problem as practice.

Problem 3.3. Find the remainder when 119^{10} is divided by 19.

§3.4 Fermat's Little Theorem

In very special scenarios, exponentials become trivial to calculate $\pmod{n}$. Knowing these scenarios can help us calculate faster. One of these scenarios is given in **Fermat's Little Theorem** (abbreviated **FLT**), stated in 2 forms below.

Theorem 3.4 (Fermat's Little Theorem, version 1)
Let p be a prime number, and let a be an integer. Then $a^p \equiv a \pmod{p}$.

Theorem 3.5 (Fermat's Little Theorem, version 2)
Let p be a prime number, and let a be relatively prime to p. Then $a^{p-1} \equiv 1 \pmod{p}$.

As an example, suppose we want to compute $3^{18} \pmod{7}$. Since 3 is relatively prime to the prime number modulus of 7, FLT tells us that $3^6 \equiv 1 \pmod{7}$. Therefore, since $3^{18} = (3^6)^3$, the desired remainder is simply $1^3 \equiv 1 \pmod{7}$.

As you can see from the above example, keeping an eye out for a prime modulus and applying FLT can save you the hassle of pattern finding. Keep this in mind as your try the following problems.

Problem 3.6. Find the remainder when 29^{25} is divided by 11.

Problem 3.7. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod{7}$.

In case you're curious, Fermat's Little Theorem was generalized by Leonhard Euler using his namesake phi function $\phi(n)$. You can find out about this important generalization in the "Further reading" section. The so-called Euler Totient Theorem is extremely useful on competitions!

§4 Further reading

In case you want to know more about modular arithmetic (and number theory in general), check out the following resources:

- David Altizio's introductory notes: `https://www.andrew.cmu.edu/user/daltizio/ModularArithmetic.pdf`
- "Introduction to Number Theory" by Mathew Crawford

- Chapter 5 of “The Art of Problem Solving, Volume 1: the Basics” by Sandor Lehoczky and Richard Rusczyk
- Chapter 23 of “The Art of Problem Solving, Volume 2: and Beyond” by Sandor Lehoczky and Richard Rusczyk

For those interested in division in modular arithmetic, Euler’s Totient Theorem, and other advanced techniques, the last reference (Chapter 23 of Volume 2) has plenty of material.

For advanced books at the AIME level and beyond, ask us in person.

§5 Problem Set

Easy Problems

1. (Paraguay Olympiad 2012) Define a list of numbers with the following properties:
   - The first number of the list is a one-digit natural number.
   - Each number (since the second) is obtained by adding 9 to the number before in the list.
   - The number 2012 is in that list.

   Find the first number of the list.

2. Using your skills in modular arithmetic, find the remainders when:

   (a) 555 is divided by 13

   (c) $156 \cdot 167$ is divided by 7

   (d) $24^{50} - 15^{50}$ is divided by 13

   (e) (iTest 2007) $1 + 2 + \ldots + 2007$ is divided by 1000

   (f) 5^{15} is divided by 128

   (g) 7^{7^7} is divided by 10

   (h) 12^9 is divided by 1000

3. (Brilliant) What is the remainder when

$$1! + 2! + \ldots + 50!$$

   is divided by 5!? (Here, $n!$ denotes the factorial function.)

4. (AHSME 1992) The two-digit integers form 19 to 92 are written consecutively to form the large integer

$$N = 192021 \ldots 909192.$$

   Suppose that 3^k is the highest power of 3 that is a factor of N. What is k?

5. (a) Prove Tricks #1 and #2 stated in Section 2.

   (b) Rigorize the proof of Trick #3 stated in Section 2 either using mathematical induction or the Binomial Theorem.

6. Prove that $2^n + 6 \cdot 9^n$ is divisible by 7 for any positive integer n.

Medium Problems

1. (Divisibility rules, revisited) Prove the following divisibility rules from elementary school!

   (a) An integer M is divisible by 9 if and only if the sum of its digits is divisible by 9.

   (b) An integer M is divisible by 2^n if and only if the integer formed by the last n digits is divisible by 2^n. ("Last" refers to the n rightmost digits.)

   (c) An integer M is divisible by 11 if and only if the "alternating sum" of the digits of M is divisible by 11. (In other words, if the decimal representation of M is $\overline{a_{k-1} \ldots a_1 a_0}$, then $a_{k-1} - a_{k-2} + a_{k-3} + \ldots$ must be divisible by 11.)

(*Hint for all parts:* suppose the decimal representation of M is $\overline{a_{k-1}\dots a_1a_0}$, where $a_0,\dots,a_{k-1}$ are the k digits of M. Use these place values to rewrite M as a sum of multiples of powers of 10.)

(*Warning:* Make sure you know what "if and only if" means! Ask if you don't.)

2. (AMC 10B 2010) A palindrome between 1000 and 10000 is chosen at random. What is the probability that it is divisible by 7?

3. (AMC 12A 2008) Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

4. Find all possible pairs of digits (a, b) such that the number $30a0b03$ is divisible by 13.

Hard Problems

1. Prove that
$$1 \cdot 3 \cdot 5 \cdots 2013 + 2 \cdot 4 \cdot 6 \cdots 2014$$
is divisible by 2015.

2. (Purple Comet HS 2013) There is a pile of eggs. Joan counted the eggs, but her count was off by 1 in the 1's place. Tom counted in the eggs, but his count was off by 1 in the 10's place. Raoul counted the eggs, but his count was off by 1 in the 100's place. Sasha, Jose, Peter, and Morris all counted the eggs and got the correct count. When these seven people added their counts together, the sum was 3162. How many eggs were in the pile?

3. (a) Prove that $3333^{4444} + 4444^{3333}$ is divisible by 7.

   (b) Prove that $5555^{2222} + 2222^{5555}$ is divisible by 7.

4. (Mandelbrot 2008-09) How many zeroes occur at the end of the number $1999^6 + 6 \cdot 1999 + 5$?

5. (AIME 1989) One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.

6. (PUMaC 2008) If $f(x) = x^{x^{x^x}}$, find the last two digits of $f(17)+f(18)+f(19)+f(20)$.

7. (Mandelbrot 2008-09) Determine the smallest positive integer m such that $m^2 + 7m + 89$ is a multiple of 77.

   (*Hint:* use the **Chinese Remainder Theorem** (**CRT**) to a system of congruences (mod 7) and (mod 11). If you don't know CRT, look it up online, check the "Further reading" section, or ask us.)