Introduction to Modular Arithmetic

1 Introduction

Modular arithmetic is a topic residing under Number Theory, which roughly speaking is the study of integers and their properties. Modular arithmetic highlights the power of remainders when solving problems. In this lecture, I will quickly go over the basics of the subject and then dive into what makes this topic so interesting. (Note that this lecture will be much more information-loaded than the previous one, in that unlike last time this will probably be an entirely new concept for most of you.)

2 Number Theory Basics

These definitions are all taken from last year's lecture. If there is anything you don't understand/remember, feel free to ask.

- It's sort of difficult to define integers in themselves, but in this case the Wikipedia definition suffices: "An **integer** is a number that can be written without a fractional or decimal component." Some examples of integers are 5, -17, and 3628800. It is important to know that while the set of integers is closed[1] under addition, subtraction, or multiplication, it is **NOT** under division!

- An integer a is said to be a **multiple** of another integer b if there exists an integer k such that $a = kb$. The integer b here is said to be called a **factor** or a **divisor**[2] of a. Furthermore, a is said to be **divisible** by b.

  If an integer has no positive divisors other than 1 and itself, it is said to be **prime**; otherwise, it is said to be **composite** (with the exception of 1, of course.)

- Any integer N can be written as the product of the primes it is divisible by. The **prime factorization** of N is

$$N = \prod_{p \in \mathbb{P}} p^{e_i} = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots,$$

  where $\mathbb{P}$ is the set of positive primes and $\{e_i\}$ is a sequence of integers determining how many times the ith prime number can be divided out of N. For example, $144 = 2^2 \cdot 3^2$ and $7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Prime factorization often plays a critical role in NT problems, so know it on the back of your hand!

- The **greatest common divisor** of a set of integers A is the largest positive integer n that divides evenly into every element in A. For example, $\gcd(15, 20) = 5$ and $\gcd(12, 18) = 6$. Similarly, the **least common multiple** of a set of integers B is the smallest positive integer N such that N is evenly divisible by every integer in B. For example, $\operatorname{lcm}(15, 20) = 60$ and $\operatorname{lcm}(12, 18) = 36$. There are formulae for these, but there is no need to go into them now.

3 Background and Notation

In one sense, we can consider the integers as never-ending, on a number line stretching from $-\infty$ to ∞. This is well-known and has been taught ever since Kindergarden. In another sense, however, the integers act in a cyclic (i.e. repeating) manner. For example, consider classifying the integers as whether they are even or odd. Then it is clear that there is a pattern that repeats every two integers: even, odd, even, odd, $\cdots$. We can extend this to form other patterns; the remainders of integers upon division by 3, for instance, follow the pattern $0, 1, 2, 0, 1, 2, \cdots$. Recognizing such patterns can help us solve problems.

Example 1. *Suppose it is* $1:00$ *now. What time will it be exactly* 1000 *hours from now?*

Solution. The key to solving this problem is realizing that the times will repeat themselves every 12 hours. This means, for example, that 12 hours from now the time will be $1:00$, 24 hours from now the time will be $1:00$, and so on. We can extrapolate this and say that the time will be $1:00$ whenever the number of hours from now is a

[1] A set A is said to be **closed** under an operation if said operation takes members from the set to produce a member from that same set. For example, multiplying two integers produces another integer.

[2] While both of these terms are usually interchangable, usually the latter one is more often used.

multiple of 12. What is the multiple of 12 that is closest to 1000? After some experimentation, we see that the closest multiple is 996, so 996 hours from now it will be $1:00$ as well. Thus, exactly 1000 hours from now the time will be $\boxed{5:00}$. ■

In the above solution, note that the answer to the question depends only on the remainder when 1000 is divided by 12, which was 4. As a result, the answer would be the same whether we were asking for the time 4 hours from now, 16 hours from now, 1000 hours from now, or 4252 hours from now.

To make the above reasoning more rigorous, we can group the integers into groups called **residue classes modulo** n that have a common remainder when divided by n, and we say two integers are **congruent** or **equivalent** modulo n if they lie in the same residue class. For example, the integers 4, 16, 1000, and 4252 all are congruent modulo 12 since they share the same remainder when divided by 12.

More formally, we say that $a \equiv b \pmod{n}$ if a and b fall in the same residue class modulo n. Thus, we can say $1000 \equiv 4 \pmod{12}$ for the reasonds discussed above. At the same time, $1000 \equiv 16 \pmod{12}$. Similarly, the statements $16 \equiv 1 \pmod{3}$, $79 \equiv 1 \pmod{11}$, and $4007 \equiv 17 \pmod{19}$ are all valid.

The idea of residue classes is strange at first, but it is important to realize that we are not saying that two integers are equal here. Rather, when we write $a \equiv b \pmod{n}$, we are suggesting that a and b belong to the same group of remainders and as such we can jump from one integer to the other freely.

4 Basic Arithmetic

Many of the rules of arithmetic apply to modular arithmetic as well. In particular, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$. This is most easily seen with a few examples.

Example 2. *What are the remainders when* $3333 + 4444$ *and* $3333 \cdot 4444$ *are divided by* 5*?*

Solution. We have $3333 \equiv 3 \pmod{5}$ and $4444 \equiv 4 \pmod{5}$, so $3333 + 4444 \equiv 3 + 4 \equiv 7 \equiv \boxed{2} \pmod{5}$. Similarly, $3333 \cdot 4444 \equiv 3 \cdot 4 \equiv 12 \equiv \boxed{2} \pmod{5}$. ■

In general, we can take any integer and replace it with an integer within the same residue class. We can do this multiple times within a problem.

Example 3. *What is the remainder when* 2015^{2015} *is divided by* 2014*?*

Solution. Note that 2015^{2015} can be rewritten as

$$\underbrace{2015 \cdot 2015 \cdot \ldots \cdot 2015}_{\text{2015 terms}}.$$

Since $2015 \equiv 1 \pmod{2014}$, when evaluating the remainder when dividing by 2014 we can replace each of these 2015's with a 1. Therefore the desired answer is $1 \cdot 1 \cdot \ldots \cdot 1 = \boxed{1}$.

Note that this solution can be shortened by replacing the 2015 with a 1 in the beginning of the problem, as follows:

$$2015^{2015} \equiv 1^{2015} \equiv \boxed{1} \pmod{2014}.$$

■

The above problem is our first glimpse into the power of modular arithmetic. No human being could ever dream of multiplying out 2015^{2015} - it's simply too computationally infeasible. Modular arithmetic helped us determine the remainder when 2015^{2015} is divided by 2014 without going through all the gory arithmetic!

Try your hand at the next problem before moving on.

Problem 1. *Is* $21^{100} - 12^{100}$ *a multiple of* 11*?*

5 A Few More Advanced Examples

Okay, now you should have the basics down a bit. (If not, stop me here, and we can do a few more exercises so that you guys get the hang of it.) Here are a few more remainder computations that are a bit more difficult to pull off. These will hopefully help you become more confidence with modular arithmetic.

Example 4. *What is the remainder when* 7^{2015} *is divided by* 48*?*

Solution. At first, it seems that even modular arithmetic can't prevent this problem from becoming messy. However, upon further inspection, we can see that $7^2 = 49$, which leaves a remainder of 1 when divided by 48! Hence, we can write

$$7^{2015} \equiv 7 \cdot (7^2)^{1007} \equiv 7 \cdot 1^{1007} \equiv \boxed{7} \pmod{48}.$$

■

Example 5. *What are the last two digits of the integer* 17^{198}*?*

Solution. Note that $17^2 \equiv 289 \equiv -11 \pmod{100}$. Thus, the problem is simplified to computing $(-11)^{99} \equiv -11^{99} \pmod{100}$. Now note that by the Binomial Theorem

$$11^{99} = (10+1)^{99} = 10^{99} + \cdots + \binom{99}{2}10^2 + \binom{99}{1}10^1 + 1.$$

When this expansion is reduced modulo 100, all but the last two terms will go away since they are all divisible by 100, so $11^{99} \equiv \binom{99}{1} \cdot 10 + 1 \equiv 91 \pmod{100}$. As a result, $17^{198} \equiv -91 \equiv \boxed{09} \pmod{100}$. ■

To check our work, we can always use WolframAlpha. Indeed, the computational powerhouse suggests that

$$\begin{aligned}17^{198} = {} & 4254871345860260773820291271704849130393265438068192609194205906081766431755337385 \\ & 3755499288972428647279052646422715030862464546452440645808440896351754510501532667 \\ & 43295026488304431966804630624591243393794658069711060298952254618629018195360609,\end{aligned}$$

which does end in the two digits 09. Hooray for math!

6 Uses for Modular Arithmetic Outside of Computation

From our work above, it seems that the only uses for modular arithmetic all relate to finding remainders for really large numbers. This is not true! Modular arithmetic is a key tool which is useful for all different aspects of Number Theory, including solving equations in integers. Here are a few problems which showcase modular arithmetic and its uses in other types of problems.

Example 6 (Divisibility Rule for Powers of Two)**.** *Note that the divisibility rule for* 2 *states that an integer is divisible by* 2 *if and only if its last digit is divisible by* 2*. Note further that the divisibility rule for* 4 *states that an integer is divisible by* 4 *if and only if the integer formed by its last two digits is divisible by* 4*. (For example,* 124564 *is divisible by* 4 *because* 64 *is divisible by* 4*.) Prove a general divisibility rule for* 2^n*: any integer is divisible by* 2^n *if and only if the integer formed by its last* n *digits is also divisible by* 2^n*.*

Solution. Let Y be the integer formed by the last n digits and let X be the integer formed by the digits to the left of these n digits. For example, in the 124564 case above, $X = 1245$ and $Y = 64$. Note that the integer can thus be written as $10^nX + Y$. Now note that $10^n \equiv (2^n)(5^n) \equiv 0 \pmod{2^n}$, so $10^nX + Y \equiv Y \pmod{2^n}$. This immediately implies the conclusion. ■

Example 7 (Divisibility Rule for Nine)**.** *Let* $N = \overline{a_0a_1a_2\dots a_n}$ *be an integer. (The bar above the previous expression suggests the variables are digits and that we are not multiplying them together.) Prove the divisibility rule for* 9*: that* N *is divisible by* 9 *if and only if*

$$a_0 + a_1 + a_2 + \cdots + a_n$$

is also divisible by 9*.*

Solution. Note that N can be written more mathematically as

$$N = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots + a_{n-1} \cdot 10 + a_n.$$

We attempt to simplify this modulo 9. The key here is to note that $10 \equiv 1 \pmod 9$. This further implies that $10^2 \equiv 1 \pmod 9$, $10^3 \equiv 1 \pmod 9$, and so on. Making all the necessary substitutions gives

$$N \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9.$$

Thus N and the sum of the digits of N give the same remainder upon division by 9, implying the conclusion. ■

Example 8 (AMC 10B 2010)**.** *A palindrome between* 1000 *and* 10,000 *is chosen at random. What is the probability that it is divisible by* 7*?*

Solution. Let $\overline{XYYX}$ be a four-digit palindrome. Note that when expanded the integer can be rewritten as $1001X + 110Y$. Note that 1001 is divisible by 7 and $110 \equiv 5 \pmod 7$, so

$$1001X + 110Y \equiv 5Y \equiv 0 \pmod 7 \implies Y \equiv 0 \pmod 7.$$

Therefore as long as Y is either 0 or 7, the resulting palindrome will be divisible by 7. There are $2 \cdot 9 = 18$ such palindromes (since $X \neq 0$) and $10 \cdot 9 = 90$ total palindromes, so the requested probability is $\frac{18}{90} = \boxed{\frac{1}{5}}$. ■

7 Problems

1. [Paraguay 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.[3]

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

   (a) 555 is divided by 13

   (b) 555^2 is divided by 13

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

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

   (e) [iTest 2007] $1 + 2 + \cdots + 2007$ 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. I am thinking of a number. All I can give to you is that if you triple my number, it leaves a remainder of 13 when divided by 17. Unfortunately, this is clearly not enough information to figure out my number. However, it is enough information to figure out what the remainder of my original number is when divided by 17. What is this remainder?

   (A) 9 **(B)** 10 **(C)** 11 **(D)** 12 **(E)** 13

   (This problem is here to help you figure out how to divide in modular arithmetic. It's not as simple as the other arithmetic operations are. As a hint, try to find a number that satisfies the given properties, and then figure out how to find the desired remainder without guess-and-check.)

[3] Yes, this actually appeared on a national olympiad. Do not ask me why.

4. Using a similar method as we did in Example 7, prove the divisibility rule for 11: if $N = \overline{a_0 a_1 a_2 \dots a_n}$ is a positive integer, then N is divisible by 11 if and only if

$$a_0 - a_1 + a_2 - \cdots + a_n(-1)^n$$

is also divisible by 11.

(Warning: at this point in the problem set, there's a huge spike in difficulty. Sorry! Modular arithmetic problems at this level are really really hard to find.)

5. Prove that

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2013 + 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2014$$

is divisible by 2015.

6. [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?

7. [Math League HS 1990-1991] The quadratic equation $ax^2+bx+c=0$ has integral coefficients, and the value of its discriminant is D. What is the smallest value of $D > 48$ for which the solutions of this quadratic equation will be irrational?[4]

(A) 49 **(B)** 50 **(C)** 51 **(D)** 52 **(E)** 53

★ 8. [Mandelbrot 2008-2009] Determine the smallest positive integer m such that $m^2+7m+89$ is a multiple of 77.

★ 9. [Mandelbrot 2003-2004] How many zeroes occur at the end of the number $1999^6 + 6 \cdot 1999 + 5$?

(A) 4 **(B)** 5 **(C)** 6 **(D)** 7 **(E)** 8

★ 10. [AMC 12B 2010] Arithmetic sequences (a_n) and (b_n) have integer terms with $a_1 = b_1 = 1 < a_2 \leq b_2$ and $a_n b_n = 2010$ for some n. What is the largest possible value of n?

(A) 2 **(B)** 3 **(C)** 8 **(D)** 288 **(E)** 2009

[4] Hint: it may help to examine the possible remainders when a perfect square is divided by 4.