Modular Arithmetic

Bohan Yao

Math Lectures Handout

"What are mods? Is it like the pizza company?" - Bohan Yao

§1 Prelude

So say you are given the classical problem, which is finding out the last digit of 3^x, where x is a large number. One method of "solving" this problem, although isn't really practical in most situations, is to just compute 3^x directly, and then take the last digit of it. However, it turns out that this takes around $O((x\log(3))^{1.58})$ time for a fixed k, using the most optimal method. Now this may not mean much to you if you do not study computer algorithms, but the point of this is that since $x^{1.58}$ grows really quickly after a while, eventually, even computers cannot handle this computation. It turns out that the world's fastest computers can handle up to around $x = 10^{10}$ before the computation is too much for even them. Now, if you have thought about this for a while, you may start noticing a pattern. The last digit repeats in an indefinite pattern of $3, 9, 7, 1$. Once you learn modular arithmetic, this problem will be instantly trivialized.

§2 Basic definitions

Definition 2.1. For positive integers x and m, we define $x \pmod m$ to mean the remainder when x is divided by m.

Example 2.2

Calculate $13 \pmod 5$

Now, it turns out that you can extend this theory to cases where x is negative. In this case, you can just add a lot of multiples of m until x becomes positive, and then you can carry out the standard method of division. Another thing we will define is called "Equivalence classes".

Definition 2.3. Let x be a positive integer, and let y be a non-negative integer that is less than x. Then let S be an infinite set of all the integers ω such that $\omega \pmod x = y$. Then we call S the *equivalence class of y mod x*. If two integers a, b are in the same equivalence class $\pmod x$, then we denote this as $a \equiv b \pmod x$. (we also call equivalence classes residue classes)

Now this may seem very dull at first, but there is actually a lot of structure behind mods that you may not have seen before. For example, consider the following:

Proposition 2.4 (Modular Theory)
The following hold about mods:
Let a, b, c, d, m be five integers such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$
$a + c \equiv b + d \pmod{m}$.
$a - c \equiv b - d \pmod{m}$. (Subtraction)
$ac \equiv bd \pmod{m}$. (Multiplication)
$a^e \equiv b^e \pmod{m}$ where e is a positive integer. (Exponentation)

Exercise 2.5. Prove Proposition 2.4 (As a hint, try to represent a, b, c, d in a way that incorporates the fact that $a \equiv b \pmod{m}$ and that $c \equiv d \pmod{m}$).

Now you may notice that division is not on there. It turns out there is a very good reason why it is not on there! Take for instance the example $\frac{6}{2} \pmod{2}$. Now its obvious to see that this evaluates to 1. However, something very bad happens if we try to apply a similar thing to what the propositions did above. Since 2 and 6 are both in the 0 equivalence class, this means that we can "reduce" the expression to $\frac{0}{0} \pmod{2}$. What. Since division by 0 is undefined, this "proposition" clearly doesn't work.
So now we have something to work upon. The next few theorems however, will totally change your opinion on modular arithmetic. I guarantee it.

§3 Powerful Theorems

Definition 3.1 (Totient)**.** We define the function $\phi(n) : \mathbb{Z} \implies \mathbb{Z}$ be the function that counts the number of positive integers less than n that are relatively prime to n.

Exercise 3.2. Find a way to computer $\phi(n)$ quicker than testing all of the integers less than or equal to n.

So this by itself does absolutely nothing. Woohoo! However, this serves as the key function for the next theorem.

Theorem 3.3 (Euler)
For any integer m and any integer a that is relatively prime to m, we have that $a^{\phi(m)} \equiv 1 \pmod{m}$.

Corollary 3.4 (Fermat)
Given a prime p and any non-zero integer a, we have that $a^{p-1} \equiv 1 \pmod{p}$

So these are the key theorems you need to know about modular arithmetic. It turns out that these two theorems are all you need to solve most number theory problems, although you also need creativity.
Well, how do you apply these theorems? Answer: More mods! Take for example, the problem from the section *Prelude*. We will show that this pattern holds in general. Notice that $3^x \pmod{1}0$ is actually the last digit of 3^x. Now we can apply Euler's Totient Theorem, as 3 and 10 are relatively prime. Computing $\phi(10) = 4$, and noticing that $3^x \equiv 3^{x-4} * 3^4 \pmod{1}0$ by exponent rules, then using $3^4 \equiv 1 \pmod{1}0$ gives us $3^x \equiv 3^{x-4} \pmod{1}0$. Now, you keep applying this until you reach the point where the

current exponent is simply $x \pmod 4$, and you can directly evaluate the last digit. This is an example of the way you generally want to apply these theorems.

Corollary 3.5

For any integer m and any integer a that is relatively prime to m, we have that $a^x \equiv a^{x \pmod{\phi(m)}} \pmod m$ for all positive integers x.

The powerful thing is that x need not be positive! You can apply Euler in reverse to bring x to a positive integer x', then use Corollary 3.5.

Now we actually need one more theorem in some cases, called the Chinese Remainder Theorem.

Theorem 3.6 (CRT)

If a_i is a sequence of pairwise relatively prime positive integers, and b_i is also a sequence of integers such that there are the same number of elements in both sequences, then there exists a positive integer x such that for any pair a_i, b_i, $x \equiv b \pmod a$

This theorem actually allows you to bypass the condition that a and m are relatively prime in Euler's theorem, as we will see soon in the problems.

§4 Problems

Example 4.1 (2011 USAJMO P1)

Find, with proof, all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.

Proof. Take the expression $\pmod 3$ and reduce the bases $\pmod 3$. Now note that squares are either $0 or 1 \pmod 3$, so you can narrow down the answers. Then take $\pmod 4$ and finish with a similar insight. □

Example 4.2 (Classic)

The number 2^{29} contains all but one of the digits from 0 to 9. Find the missing digit.

Proof. Prove that a number is congruent $\pmod 9$ to the sum of its digits by considering the number in expanded form. Then just find $2^{29} \pmod 9$ by Euler and compare to $0 + 1 + 2 + \cdots + 9 \pmod 9$. □

Example 4.3 (Mathcounts?)

Find the remainder when 2019^{2020} is divided by 2020.

Proof. The key to this problem is using $2019 \equiv -1 \pmod{2020}$, after which it suffices to note that $(-1)^x$ is 1 for x even. □

Example 4.4 (2018 AMC 8 P21)

How many positive three-digit integers have a remainder of 2 when divided by 6, a remainder of 5 when divided by 9, and a remainder of 7 when divided by 11?

Proof. Since we cannot apply CRT right away, as 6 and 9 are not relatively prime, we look for other options. However, you can just "decompose" the $\pmod 6$ into $\pmod 2$ and $\pmod 3$, after which applying CRT works. □

Example 4.5 (2018 AMC 10B P 16)

Let $a_1, a_2, \ldots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$

What is the remainder when $a_1^3 + a_2^3 + \cdots + a_{2018}^3$ is divided by 6?

Proof. You can verify that $a^3 \equiv a \pmod 6$ for all a, and then it suffices to compute $2018^{2018} \pmod 6$, which can be done by CRT and then Euler. □

§5 Problems

Solve at least 10♣ worth of problems. As said before, all problems will involve ideas from the lecture, but solutions that do not relate to ideas from the lecture are also welcome.

My email is *solver1104@gmail.com*. Please write up a brief sketch of your solutions and send them to me.

Problem (2♣, 2012 AMC 8 P12)**.** What is the units digit of 13^{2012} ?

Problem (2♣, Own)**.** What is the smallest number x such that $x \equiv 3 \pmod 5$, $x \equiv 10 \pmod 1$1, and $x \equiv 3 \pmod 1$3?

Problem (2♣, Own)**.** What are the last three digits of the number 162^{202}?

Problem (3♣, Classic?)**.** What is the last digit of the number $2^{2^{2^{\cdots}}}$, where there are 10000 2s?

Problem (3♣, Modified version of 2011 AMC 10 P23)**.** What are the last three digits of the number 2011^{2011}?

Problem (3♣, 2014 AMC 10B P17)**.** What is the greatest power of 2 that is a factor of $10^{1002} - 4^{501}$?

Problem (5♣ AIME?)**.** How many numbers from 1 to 1000 are there such that the number, when divided by 7, does not have a remainder of 0, 1, or 6, when divided by 11, does not have a remainder of 0, 1, or 10, and when divided by 13, does not have a remainder of 0, 1, or 12?

Problem (7♣, 2003 Canada Olympiad Problem 2)**.** Find the last three digits of the number $2003^{2002^{2001}}$

Problem (7♣, 1983 AIME I P6)**.** Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.

Problem (10♣, JBMO 1997 Problem 5)**.** Let n_1, n_2, …, n_{1998} be positive integers such that

$$n_1^2 + n_2^2 + \cdots + n_{1997}^2 = n_{1998}^2.$$

Show that at least two of the numbers are even.

Problem (10♣, 2018 AIME I P11)**.** Find the least positive integer n such that when 3^n is written in base 143, its two right-most digits in base 143 are 01.