Mods

Julian Zhang

March 2021

1 Introduction

This handout is a continuation of the handout on Number Theory from last week. Modular arithmetic is an interesting concept to think about, especially if you want to pursue a career in pure number theory or computer science. Special thanks go out to Pierre de Fermat, and Eric Shen (who a lot of this was taken from), what else is new?

2 Definitions

Lets consider any two numbers x and y, and a certain number n. We know that for all such x, n divides x if and only if the remainder upon division is equal to 0. In addition, if n divides both x and y, then since they are both multiples of n, both $x+y$ and $x-y$ will also be multiples of n, and thus divisible by n. So will any combination $ax+by$, where a and y are integers. But let's say we want to consider when x and y are not divisible, yet $x+y$ is. How could we keep track of this?

Well, let's try representing x and y with their remainders in mind. More specifically, let's set:

$$x = an + b$$
$$y = cn + d$$

where b and d are the remainders upon division. Now, we have that $x+y = (a+c)n+b+d$. Thus, $x+y$ is divisible by n if and only if $b+d$ is - and $b+d$ can be treated as "more or less" a remainder, give or take an n (note that if they're both equal to $n-1$ then $b+d$ is equal to $2n-2$, which is usually bigger than n. Keep in mind this little annoyance).

Anyhow, this means that there's some "well-behavedness" here: we have that the remainder of $x+y$ upon division is *basically* equal to the sum of the remainders of x and y. Let's try this out also for, say, multiplication. Again represent x and y in their previous forms: then we have that xy satisfies:

$$\begin{aligned} xy &= (an+b)(cn+d) \\ &= (acn + bc + ad)n + bd \end{aligned}$$

Again, we have that the "remainder"-ish here is bd where xy is divisible by n iff xy is. It would be the remainder if bd were small enough, but unfortunately there's a little bit of a size issue there. But coming back, we again have this mysterious property that the product of the remainders of x and y serves as a remainder-ish for xy. Eventually, mathematicians got tired of writing things as remainders, and defined something to make writing them easier:

Definition: Given $x = an + b$, we say would say that "x divided by a leaves a remainder of b". In modular notation, we define

$$x \equiv a \bmod b$$

We pronounce this as "x is congruent to a, [when taken] mod[ulo] b"

Using this new definition, we can now re-write the previous properties using mods.

ADDITION: If $x \equiv a \bmod n$, and $y \equiv b \bmod n$, then:

$$x + y \equiv a + b \bmod n$$

MULTIPLICATION: If $x \equiv a \bmod n$, and $y \equiv b \bmod n$, then:

$$xy \equiv ab \bmod n$$

NOTE: it's important to remember that this $\equiv$ does not mean "equal" but rather "is equivalent to". There are no "equalities" in modular arithmetic - only such equivalences, so make sure to remember that distinction.

Since all you guys really care about are contests though, here's a list of most useful mod properties:

Theorem: **Mod Properties:** Let $a \equiv b (\bmod n)$, and c be a positive integer. Then,

(a) $a + c \equiv b + c \pmod n$

(b) $a - c \equiv b - c \pmod n$

(c) $ac \equiv bc \pmod n$

(d) $a^c \equiv b^c \pmod n$

(e) $a + b \equiv (a \bmod n) + (b \bmod n) \pmod n$

(f) $ab \equiv (a \bmod n)(b \bmod n) \pmod n$

(g) If $\gcd(c, n) = 1$ and $dc \equiv ec \pmod n$, then $d \equiv e \pmod n$

(h) if $k|a, k|b$, and $k|n$, then $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{n}{k}}$

3 Usefulness

This is probably self evident, but whenever a question tells you to "find the remainder when", it most likely involves mods.

3.1 really really big numbers

When you were younger, you've probably seen something like the following in a math contest:

Example 1 (every 4th grade contest)

Compute the units digit of $123512351351235 \cdot 34895783758912375$

Solution: Just take the last two digits and multiply them. This gives us 25, so 5 is our desired units digit. Without noticing it, this is just working in mod 10! Now, let's try working in different mods

Example 2 (big scary number)

Determine the remainder when 2019^{2019} is divided by 2018.

We have:

$$\begin{aligned} 2019^{2019} &\equiv 1^{2019} \\ &\equiv 1 \bmod 2018 \end{aligned}$$

Thus the remainder is one.

Example 3 (more scary number)

Prove that $200^5 - 11^5$ is divisible by 9.

We have:

$$\begin{aligned} 200^5 - 11^5 &\equiv (11 + 189)^5 - 11^5 \\ &\equiv 11^5 - 11^5 \\ &\equiv 0 \bmod 9 \end{aligned}$$

Basically this gives us that when divided by 9 the difference leaves no remainder, and thus the difference is indeed divisible by 9 as desired.

3.2 Divisibility Rules

You probably already know the divisibility rules for 1-11, but let's try proving some of them, starting with 9. It essentially states that if a number $\overline{a_n a_{n-1} \dots a_0}$ is divisible by 9, then the sum of its digits must be divisible by 9 as well.

PROOF: Note that for any k, we have that $10^k \equiv 1^k \equiv 1 \bmod 9$. Now, we have:

$$\begin{aligned} \overline{a_n a_{n-1} \dots a_0} &= a_n 10^n + a_{n-1} 10^{n-1} + \dots a_0 \\ &\equiv a_n + a_{n-1} + \dots a_0 \end{aligned}$$

Since a number is equivalent to the sum of its digits mod 9, one of them being divisible by 9 means that the other must be divisible by 9 as well, as desired.

NOTE: The proof for the divisibility rule of 3 is now trivial, since you just need to notice that $10 \equiv 1 \pmod 3$, and the statements become the same.

Now, let's prove the rule for 11. A number $\overline{a_n a_{n-1} \dots a_0}$ is divisible by 11 if the alternating sum of it's digits, or $a_0 - a_1 + a_2 \dots + (-1)^n (a_n)$ is divisible by 11.

PROOF: Note that $11 \equiv -1 \bmod 10$. We then have:

$$\begin{aligned}\overline{a_n a_{n-1} \dots a_0} &= a_n 10^n + a_{n-1} 10^{n-1} + \dots a_0 \\ &\equiv a_n (-1)^n + a_{n-1}(-1)^{n-1} + \dots a_0\end{aligned}$$

Which is the same thing as the alternating sum of digits. Now, the divisibility rules of 9 and 11 can actually be generalized to any base n, because we currently operate in decimal (base-10).

Theorem: i thought of this and its actually quite cool

Given a number $x = \overline{a_k a_{k-1} \cdots a_0} = a_k n^k + a_{k-1} n^{k-1} + \cdots a_0$, in base n:

1. $n-1 \mid x$ if and only if $n-1 | a_0 + a_1 + \dots + a_k$ (sum of digits)
2. $n \mid x$ if and only if $a_0 = 0$
3. $n+1 \mid x$ if and only if $n+1 | a_0 - a_1 + \dots + (-1)^k a_k$ (alternating sum)

In fact, I'm pretty sure this can actually even be generalized to factors of $n-1$ and $n+1$.

3.3 Diophantine Equations

To recall, these are equations of the form

$$ax + by = c$$

In the number theory handout we covered these, but they can also be simplified using mods. Whenever we want to find integer x, y that satisfy this equation, it's always good to look for mods. In particular, $(\bmod a)$ and $(\bmod b)$ are good places to start, as they take out one term each. We'll take $(\bmod b)$ here, giving us

$$ax \equiv c \bmod b$$

We now technically just have to go through all b (or less, if $\gcd(a, b) > 1$) possibilities for ax, and see if one (or none) of them equal to c.

Once we've found all our solutions within the mod, we can add b to x and subtract a from y, and since this preserves their sum we can get the infinite families of solutions to this equation in integers by adding or subtracting b from x and shifting y accordingly.

Note that it's always better to take the **smaller** mod, as this gives you less cases to check.

Here's an example:

Problem: Solve in integers $3x + 5y = 7$.

Solution: We take mod 3, giving us that:

$$\begin{aligned}5y &\equiv 7 \bmod 3 \\ 2y &\equiv 1 \bmod 3\end{aligned}$$

This gives us that we must have y is equivalent to 2 mod 3.

Now, express $y = 3k+2$. Solving for x gives that $x = -1-5k$, and thus our solution set is $(-1-5k, 3k+2)$ for all integers k.

4 Prime Mods

Note how in the previous list of properties of mods, there wasn't one for division. Say you were working mod n, and trying to divide by some m which shared a common factor with n. You can't really divide mods in the case that one of them is reductible and the other isn't, in other words, if the mod you're working in is composite.

Conversely though, there are actually a number of special properties that hold true if you're working in a prime mod. Prime mods, unlike composite mods provide a closed structure, so here are some theorems that take advantage of that:

> **Theorem: Fermat's Little Theorem:**
>
> Let p be a prime number, and a be an integer such that $\gcd(a, p) = 1$. We have that:
>
> $$a^{p-1} \equiv 1 \bmod p$$

PROOF: Let's consider the integers 1, 2, $\ldots p-1$. Note that all of these have distinct residues mod p.

Now, let's say we multiply all of these by a. Then we get the integers a, $2a$, $\ldots (p-1)a$. Still, none of them are divisible by p because a and p are relatively prime by definition.

Now, let's assume that two of them (ia and ja) are equivalent mod p. Then this would give us that:

$$ia - ja \equiv 0 \bmod p$$
$$p|(i-j)a$$

However, both i and j are in between 1 and $p-1$ (inclusive), so this is impossible unless $i = j$ (and so they're the same number).

This means that we have $p-1$ residues that these new integers can take, and they all have to be in different residues. Thus, all $p-1$ residues must be taken, and thus a, $2a$, $\ldots (p-1)a \pmod p$ are the same as 1, 2, $\ldots p-1 \pmod p$, but rearranged. If that's the case, then their products should also be the same:

$$a \cdot 2a \ldots \cdot (p-1)a \equiv 1 \cdot 2 \ldots \cdot p-1 \bmod p$$

Dividing by $(p-1)!$ on both sides gives us

$$a^{p-1} \equiv 1 \bmod p$$

as desired!

One more important result would be Wilson's theorem, presented below:

> **Theorem: Wilson's Theorem**
>
> For any prime number p, we have that
>
> $$(p-1)! \equiv 1 \bmod p$$

PROOF: Recall that since we're under a prime mod, properties of division work. Looking at $(p-1)!$,

we know that for any a not divisible by p, there exists a residue b such that:

$$ab \equiv 1 \bmod p$$
$$b \equiv \frac{1}{a} \bmod p$$

This is known as the **inverse** of p.

This means that we can pair *most* of the numbers in $(p-1)!$ to be equivalent to 1. But the numbers that we can't pair up actually have themselves as the inverse! This would just be 1 and -1, so thus we have that:

$$\begin{aligned}(p-1)! &\equiv 1 \cdot -1 \bmod p \\ &\equiv -1 \bmod p\end{aligned}$$

as desired!

5 Problems

This is yoinked directly from Eric: Point weights are given. Try to get at least $\boxed{25}$ points. Questions marked with red are mandatory.

1. (6) A bit of practice with mods: Find the remainder!
   (a) 7^6 divided by 6
   (b) 253^4 divided by 64
   (c) 1999^{1000} divided by 1000
   (d) $203^{17} - 287^{17}$ divided by 14
   (e) $47^8 - 37^8$ divided by 7.
   (f) $7^{28} - 6^{14}$ divided by 43
   (g) 2^{2001} divided by $2^7 - 1$
   (h) 7^{7^7} divided by 10
2. (3) In how many ways can 1776 identical flags be partitioned into piles of either three or four flags so that every flag is in some pile?
3. (3) Compute the tens digit of $1! + 2! + \ldots 100!$.
4. (3) Claudia has 12 coins, each of which is a 5-cent coin or a 10-cent coin. There are exactly 17 different values that can be obtained as combinations of one or more of her coins. How many 10-cent coins does Claudia have?
   (A) 3 **(B)** 4 **(C)** 5 **(D)** 6 **(E)** 7
5. (3) Al and Barb start their new jobs on the same day. Al's schedule is 3 work-days followed by 1 rest-day. Barb's schedule is 7 work-days followed by 3 rest-days. On how many of their first 1000 days do both have rest-days on the same day?
   (A) 48 (B) 50 (C) 72 (D) 75 (E) 100
6. (4) Let n be an integer. If the tens digit of n^2 is 7, what is its units digit?

7. (3) Find the remainder when $1^3 + 2^3 + \ldots 100^3$ is divided by 9.

8. (4) What is the remainder when $10^{20^{30}}$ is divided by 13?

9. (6) An arithmetic sequence is defined as a sequence of numbers where the difference between any two consecutive terms is a constant. For example, $1, 3, 5, \cdots$ is an arithmetic sequence. In addition, let a non-increasing integer be defined as an integer such that every digit is less than or equal to each digit to the left. For example, 87753 is non-increasing but 85722 is not. Prove that there are infinitely many non-increasing integers in the arithmetic sequence $11, 20, 29, \cdots$.

10. (4) What is the hundreds digit of 2011^{2011}?

11. (4) If there exists four distinct primes for which the sum of any three is a prime number, find the minimum possible value of the smallest prime out of the four.

12. (6) For all integers $1 \leq n \leq 18$, define $f(n)$ to be the smallest positive integer k such that nk is congruent to either 1 or 18 modulo 19. Compute:

$$\sum_{n=1}^{18} f(n)$$

13. (9) The sequence (x_n) is defined by $x_0 = 1$ and $x_{n+1} = 2022^n + x_n$ for all $n \geq 0$. Compute x_{2020} mod 100.

14. (14) Let $q = \frac{3p-5}{2}$ where p is an odd prime, and let

$$S_q = \frac{1}{2 \cdot 3 \cdot 4} + \frac{1}{5 \cdot 6 \cdot 7} + \cdots + \frac{1}{q(q+1)(q+2)}$$

Prove that if $\frac{1}{p} - 2S_q = \frac{m}{n}$ for integers m and n, then $m - n$ is divisible by p.