Computational Number Theory

Vidur Jasuja

November 2020

1 So what is a mod anyway?

1.1 Some Notes

- Note: unless stated otherwise, all variables stated will be assumed to be integers.
- If a is divisible by b, we say that b divides a, denoted as $b \mid a$.

1.2 Defining Congruence

Definition (Congruence $\pmod n$)

We say two numbers a and b are congruent modulo n, where n is positive, or $a \equiv b \pmod n$, if any one of the equivalent conditions listed here are met.

- If n divides the difference of a and b, or in other words n divides $a - b$;
- If there exists an integer k such that $a + kn = b$;
- Or if a and b leave the same remainder upon division by n.

Can you explain why these conditions are equivalent?

§1.2.1 Simple Exercises

1. Find a number n such that $n \equiv 2020 \pmod{64}$.
2. Find a number n such that $n \equiv -27 \pmod{46}$.
3. Find a number $0 \leq n < 57$ such that $n \equiv 982 \pmod{57}$. What is another way to phrase this problem in more simple terms?
4. How many positive integers m are there such that $50 \equiv 2 \pmod m$?

1.3 Properties of Mods

Theorem (Addition works $\pmod n$)

Suppose that $a \equiv b \pmod n$, and $c \equiv d \pmod n$. Then $a + c \equiv b + d \pmod n$.

Proof

By our definitions of congruence, we have that $b = a + nj$ for some integer j, and that $d = c + nk$ for some integer k.

Now, by our other equivalent definition of congruence, we want to show that $n \mid b + d - a - c$, or that

$n = c+nk+a+nj-c-a = nk+nj = n(k+j)$. Clearly, n divides $n(k+j)$, which is an integer multiple of n, so we have shown what we wanted to show.

- Can you repeat the same argument for showing that subtraction and multiplication hold $\pmod m$?

§1.3.1 Modular Arithmetic Exercises

We have shown that addition, subtraction, and multiplication work modulo m; that is, we can do arithmetic modulo m (except division, which we will address later). What this means is that if you have some equation involving just these operations, you can substitute any two congruent things for one another.

1. Find the remainder when 5^{15} is divided by 7.
2. Suppose that m leaves a remainder of 3 when divided by 20, n leaves a remainder of 6 when divided by 20, p leaves a remainder of 9 when divided by 20, and q leaves a remainder of 13 when divided by 20. What is the remainder when $(m+n)(p+q)$ is divided by 20?
3. Suppose that $a \equiv b \pmod n$. Show that $a^k \equiv b^k \pmod n$ for any integer k.
   - Show that $a-b \mid a^k - b^k$ for any integer k.
4. Show that the divisibility rules for 9 and 11 hold. (Hint: for an integer $n = \overline{a_k a_{k-1} ... a_1 a_0}$, where the $a_i's$ are digits, write n as $10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_0$, and then consider the previous problem.)
5. Find an integer k, without guessing and checking, such that $13k \equiv 1 \pmod{49}$.
6. Do the same for the congruence $19x \equiv 2 \pmod{40}$.

1.4 Fundamental Lemma

Lemma 1 (Fundamental Lemma)

Suppose n and a are relatively prime, i.e. they share no common divisors other than 1. Then if $n \mid a \cdot b$ for some b, $n \mid b$.

We will not prove this, due to the fact that the proof is annoying and involved. However, this theorem has some important applications.

§1.4.1 Exercises on the Fundamental Lemma

1. (Euclid's Lemma) Using the Fundamental lemma, show that for a prime p, if $p \mid ab$ for integers a, b, then $p \mid a$ or $p \mid b$.
2. Using the Fundamental lemma, show that if a is relatively prime to n, then no two of the n numbers $a, 2a, 3a, ..., na$ are congruent modulo n.
   (a) However, there are only n possible values of an integer modulo n - 1, 2, 3, $\ldots$, n. What does this imply about the sets $\{a, 2a, 3a, \ldots, na\}$ and $\{1, 2, 3, \ldots, n\}$ when considered modulo n?
   (b) From your conclusions about these sets, show that if a and n are relatively prime, there exists an integer b such that $ab \equiv 1 \pmod n$. This integer b is called the *inverse* of $a \pmod n$.
   (c) Conversely, show that if an integer a has an inverse modulo n, a and n share no common factors. (Hint: suppose there is a common divisor d, and show d must be 1.)
   (d) Find the inverse of $7 \pmod{10}$.
   (e) Find the inverse of $15 \pmod{23}$.
   (f) Find the inverse of $49 \pmod{77}$.

1.5 Fractional Mods

Definition

The inverse of a modulo n, where a and n are relatively prime, is the unique integer b (modulo n) satisfying the congruence $ab \equiv 1 \pmod{n}$.

The above is just what we stated earlier in fancy LaTeX.

Definition

Suppose b is relatively prime to n. Then we say that the fraction $\frac{a}{b} \pmod{n}$ is equivalent to the integer k such that $kb \equiv a \pmod{n}$.

Note that the condition that b is relatively prime to n is crucial; otherwise, there may not exist such a k, or such a k might not be unique.

§1.5.1 Exercises on Fractional Mods

1. Convince yourself that you can add, subtract, and multiply fractions modulo n just as you can integers. Make sure to not use circular reasoning - do not treat the fractions as integers! (That is, in the case of addition, for example, if $\frac{a}{b} \equiv k \pmod{n}$ and $\frac{c}{d} \equiv j \pmod{n}$, where k and j are integers, then $\frac{a}{b} + \frac{c}{d} \equiv k + j \pmod{n}$.)
2. Compute $\frac{3}{5} \pmod{7}$.
3. Compute $\frac{3}{17} \pmod{23}$.
4. Suppose that $19x \equiv 4 \pmod{29}, 2y \equiv 1 \pmod{29}$, and $2z \equiv 3 \pmod{29}$. Find the remainder when $z(x+y)$ is divided by 29. (Hint: don't bash out x, y, z.)

2 Problems

So now we have the fundamental tools of modular arithmetic - addition, subtraction, multiplication, and (limited) division.

1. (PUMaC) What is the 22nd (smallest) positive integer n such that 22^n ends in a 2?
2. (PUMaC) Find the number of positive integers $n < 2018$ such that $25^n + 9^n$ is divisible by 13.
3. Suppose that $\gcd(x, y)$ is the greatest integer dividing both x and y. Then:
   (a) $\gcd(\frac{x}{\gcd(x,y)}, \frac{y}{\gcd(x,y)}) = 1$.
   (b) If $xa \equiv xb \pmod{y}$, then $a \equiv b \pmod{\frac{y}{\gcd(x,y)}}$
4. (Modified AOIME 2020) Find the sum of all positive integers n such that when $n^2(n+1)^2$ is divided by $n + 5$, the remainder is 68.
5. (Modified CMIMC 2016) Determine the smallest positive prime p which satisfies the congruence
$$p + \frac{1}{p} \equiv 25 \pmod{83}$$
($\frac{1}{p}$ is defined as you would expect it to be.)
6. (Hard - CMIMC 2017) Find the largest positive integer N satisfying the following properties:
   - N is divisible by 7;
   - Swapping the ith and jth digits of N (for any i and j with $i \neq j$) gives an integer which is not divisible by 7.