Discussion 3A Recap

Tyler Zhu

February 18, 2020

1 Modular Arithmetic

Definition 1. We say that a is *congruent* to $b \pmod{m}$ if

$$a \equiv b \pmod{m} \iff m|a-b \iff a-b = m \cdot k, \quad k \in \mathbb{Z}.$$

One interpretation is that mod m gets the remainder when we divide by m, but the mod operator is more powerful than just that. For example, we have that

$$\begin{aligned}
\cdots \equiv -9 \equiv -4 \equiv \boxed{1} \equiv 6 \equiv 11 \equiv \dots \pmod{5} \\
\cdots \equiv -8 \equiv -3 \equiv \boxed{2} \equiv 7 \equiv 12 \equiv \dots \pmod{5} \\
\cdots \equiv -7 \equiv -2 \equiv \boxed{3} \equiv 8 \equiv 13 \equiv \dots \pmod{5}
\end{aligned}$$

Given that so many numbers are equivalent to each other when working over a certain modulus, it helps us to agree upon a set of *representatives* for each equivalence class of numbers. In the above example, the representatives for each class has been boxed. In general, the representatives are $\{0, 1, \dots, m-1\}$.

To drive this point home, compare to how we say that all of the following fractions are the same, but we use the boxed one as their representative (namely $\frac{1}{3}$):

$$\cdots = \frac{-3}{-9} = \frac{-2}{-6} = \frac{-1}{-3} = \boxed{\frac{1}{3}} = \frac{2}{6} = \frac{3}{9} = \dots$$

Doing math over a modulus is similar to normal arithmetic; addition, subtraction, multiplication, and exponentiation all hold.

Division is tricky however. Being able to divide by a is equivalent to having an *inverse*, i.e. a number x which makes $ax \equiv 1 \pmod{m}$. The existence of an inverse is equivalent to having a solution (x, k) over integers to the equation $ax = 1 + m \cdot k$. We saw in the notes (and you can reason why) that this happens only when $\gcd(a, m) = 1$, and is unique mod m.

In general, it's a good question to ask when we have solutions to the equation

$$ax + by = c$$

for $a, b, d \in \mathbb{Z}$. If we let $d = \gcd(a, b)$, then solutions exist only when $d|c$ (take this equation mod d if you don't believe me). Additionally, mod a or b these solutions are unique.

We even have an algorithm called the *Extended Euclidean Algorithm* which helps us find solutions to $ax + by = d$, from which we can get solutions to any equation in the above form (the Euclidean Algorithm lets us compute $\gcd(a, b)$ efficiently; you can imagine why extending it lets us recover the above solutons).

One common followup is finding the number of solutions to an equation like $10x \equiv 25 \pmod{30}$. Think about this (you may find the above context helpful).

2 Tips

- "Find the last digit" ⇒ Take mod 10. "Last two digits" ⇒ Take mod 100, and so on.
- It's useful to write a number n as $n = \sum_{i=0}^{k} d_i 10^i = \overline{d_k d_{k-1} \dots d_1 d_0}$ when taking mods.
- Recall that $a \equiv b \implies a^n \equiv b^n \pmod{n}$; in other words, reduce the bases of your powers.
- It can be helpful to work with different definitions of modular arithmetic. For example, showing that $3x \equiv 10 \pmod{21}$ has no solutions is easiest by demonstrating that $3x = 10 + 21k$ reduces to $0 \equiv 1 \pmod{3}$.
- While the EEA is great, finding inverses will often be faster/easier by writing out multiples of m. For example, if I'm finding the inverse of 9 mod 11, it's easier to look for a multiple of 9 in $1, 12, 23, 34, 45, \dots$ and then divide than to do the EEA.

3 Extra Practice

Exercise 3.1. Prove that for any number n, the alternating sum of the digits of n, i.e. $d_0 - d_1 + d_2 - \dots$, is divisible by 11 if and only if n is divisible by 11.