CS 70 Discrete Mathematics and Probability Theory
Spring 2020

DIS 3A

1 Party Tricks

You are at a party celebrating your completion of the CS 70 midterm. Show off your modular arithmetic skills and impress your friends by quickly figuring out the last digit(s) of each of the following numbers:

(a) Find the last digit of 11^{3142}.

(b) Find the last digit of 9^{9999}.

2 Divisible or Not

(a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, '23xx' is divisible by 4 if and only if the number 'xx' is divisible by 4.)

(b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

3 Extended Euclid: Two Ways

In this problem, we will explore the Extended Euclid's Algorithm: first, the traditional implementation, and second, a faster, iterative version. Both ways yield the same result.

Parts (a) and (b) explore the traditional Extended Euclid's Algorithm. The bolded numbers below keep track of which numbers appeared as inputs to the gcd call. Remember that we are interested in writing the GCD as a linear combination of the original inputs, so we don't want to accidentally simplify the expressions and eliminate the inputs.

(a) Note that x mod y, by definition, is always x minus a multiple of y. So, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a combination of the previous two, like so:

$$\begin{aligned}
\gcd(54,17) &= \gcd(17,3) && [\mathbf{3} = 1\times\mathbf{54} + (-3)\times\mathbf{17}]\\
&= \gcd(3,2) && [\mathbf{2} = 1\times\mathbf{17} + ____\times\mathbf{3}]\\
&= \gcd(2,1) && [\mathbf{1} = 1\times\mathbf{3} + ____\times\mathbf{2}]\\
&= \gcd(1,0) && [\mathbf{0} = 1\times\mathbf{2} + ____\times\mathbf{1}]\\
&= 1.
\end{aligned}$$

(Fill in the blanks)

(b) Recall that our goal is to fill out the blanks in

$$1 = \_\_\_\_\times\mathbf{54} + \_\_\_\_\times\mathbf{17}.$$

To do so, we work back up from the bottom, and express the gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned}
1 &= 1\times\mathbf{1} + 1\times\mathbf{0} = 1\times\mathbf{1} + (1\times\mathbf{2} + (-2)\times\mathbf{1})\\
&= 1\times\mathbf{2} - 1\times\mathbf{1}\\
&= ____\times\mathbf{3} + ____\times\mathbf{2}
\end{aligned}$$

[*Hint*: Remember, $\mathbf{1} = 1\times\mathbf{3} + (-1)\times\mathbf{2}$. Substitute this into the above line.]

$$\begin{aligned}
&= ____\times\mathbf{17} + ____\times\mathbf{3}\\
&= ____\times\mathbf{54} + ____\times\mathbf{17}
\end{aligned}$$

(c) In the previous parts, we used a recursive method to write $\gcd(54,17)$ as a linear combination of 54 and 17. We can also compute the same result iteratively - this is an alternative to the above method that is oftentimes faster. We begin by writing equations for our initial arguments, 54 and 17, as a linear combination of themselves:

$$\begin{aligned}
54 &= 1\times\mathbf{54} + 0\times\mathbf{17}\\
17 &= 0\times\mathbf{54} + 1\times\mathbf{17}
\end{aligned}$$

We can then use these initial equations to iteratively write reduced values as linear combinations of 54 and 17, until we are able to write an equation for $\gcd(54,17)$, as desired. For example, we can write:

$$3 = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17}$$

[*Hint*: $3 = 1 \times \mathbf{54} - 3 \times \mathbf{17}$. Substitute our equations for the initial arguments into this equation, and simplify.]

$$2 = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17}$$
$$1 = \_\_\_\_ \times \mathbf{54} + \_\_\_\_ \times \mathbf{17}$$

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 54?

4 Modular Arithmetic Equations

Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $9x \equiv 1 \pmod{11}$.

(b) $3x + 15 \equiv 4 \pmod{21}$.

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.