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}.

Solution:

(a) First, we notice that $11 \equiv 1 \pmod{10}$. So $11^{3142} \equiv 1^{3142} \equiv 1 \pmod{10}$, so the last digit is a 1.

(b) 9 is its own multiplicative inverse mod 10, so $9^2 \equiv 1 \pmod{10}$. Then

$$9^{9999} = 9^{2(4999)} \cdot 9 \equiv 1^{4999} \cdot 9 \equiv 9 \pmod{10},$$

so the last digit is a 9.

Another solution: We know $9 \equiv -1 \pmod{10}$, so

$$9^{9999} \equiv (-1)^{9999} \equiv -1 \equiv 9 \pmod{10}.$$

You could have also used this to say

$$9^{9999} \equiv (-1)^{9998} \cdot 9 \equiv 9 \pmod{10}.$$

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.

Solution:

(a) Using modular arithmetic, we can prove both directions of the implication at once. Take n, which has k digits.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = \sum_{i=0}^{k-1} 10^i n_i$$

We can take $n \pmod 4$ and see that all terms n_2 up to n_{k-1} drop out since $10^2, 10^3, \ldots, 10^{k-1}$ are all divisible by 4.

$$n \equiv n_0 + 10n_1 \pmod 4$$

$n_0 + 10n_1$ is 0 in mod 4 if and only if n is 0 in mod 4, proving that the number formed by the last digits is divisible by 4 if and only if the entire number n is divisible by 4.

Let us now consider the alternative solution, where we do not use modular arithmetic.

Alternative Solution

Let P be "the last two digits of n are divisible by 4", and Q be "n is divisible by 4".

Forward Direction: $P \implies Q$

Let us re-express any number n as a function of its digits. We know that the number will thus have the following value, for some k-digit number.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1}$$

We know that since 10^2 is divisible by 4, $10^2 n_2$ is divisible by 4 for all possible values of n_2. This is true for all $n_3, \ldots, n_{k-1}$. Since the number formed by the first two digits $n_0 + 10n_1$ is divisible by 4, n is divisible by 4.

Reverse Direction: $Q \implies P$

If n is divisible by 4, we can re-express $n = 4l$ for some integer l. We wish to prove that this implies the last two digits are divisible by 4. We see

$$n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = 4l.$$

Re-arrange, and we have

$$\frac{n_0 + 10n_1}{4} + 25n_2 + 250n_3 + \cdots + 25 \cdot 10^{k-3} n_{k-1} = l.$$

Since l is an integer, and all values after the first two terms are integers, we have that $(n_0 + 10n_1)/4$ is necessarily an integer. This implies that 4 divides $n_0 + 10n_1$.

(b) We will again use modular arithmetic to prove both directions of the implication at once. We will show that the condition that n is divisible by 3 is equivalent to condition that the sum of n's digits is divisible by 3.

Consider the following expression for n.

$$n = \sum_{i=0}^{k-1} 10^i n_i \pmod 3$$

Note that in mod 3, $10 = 1$, so in mod 3, this is equivalent to

$$n \equiv \sum_{i=0}^{k-1} n_i \pmod 3.$$

As it turns out, the latter expression is exactly the sum of all the digits in n. As a result, n is 0 in mod 3 if and only if the sum of all the digits is 0 in mod 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 $x \bmod y$, 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:

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

(Fill in the blanks)

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

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

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:

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

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

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

(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:

$$54 = 1 \times \mathbf{54} + 0 \times \mathbf{17}$$
$$17 = 0 \times \mathbf{54} + 1 \times \mathbf{17}$$

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?

Solution:

(a) -5

-1

-2

(b) $1 = 1 \times \mathbf{2} - 1 \times (1 \times 3 - 1 \times 2) = -1 \times \mathbf{3} + 2 \times \mathbf{2}$

$1 = -1 \times \mathbf{3} + 2 \times (1 \times \mathbf{17} + -5 \times \mathbf{3}) = 2 \times \mathbf{17} - 11 \times \mathbf{3}$

$1 = 2 \times \mathbf{17} - 11 \times (1 \times \mathbf{54} + (-3) \times \mathbf{17}) = -11 \times \mathbf{54} + 35 \times \mathbf{17}$

(c)

$$3 = 1 \times \mathbf{54} + (-3) \times \mathbf{17}$$

$$\begin{aligned} 2 &= 1 \times \mathbf{17} - 5 \times \mathbf{3} \\ &= 1 \times (0 \times \mathbf{54} + 1 \times \mathbf{17}) - 5 \times (1 \times \mathbf{54} + (-3) \times \mathbf{17}) \\ &= -5 \times \mathbf{54} + 16 \times \mathbf{17} \end{aligned}$$

$$\begin{aligned} 1 &= 1 \times \mathbf{3} - 1 \times \mathbf{2} \\ &= 1 \times (1 \times \mathbf{54} + (-3) \times \mathbf{17}) - 1 \times (-5 \times \mathbf{54} + 16 \times \mathbf{17}) \\ &= 6 \times \mathbf{54} + -19 \times \mathbf{17} \end{aligned}$$

(d) We get that the multiplicative inverse of 17 mod 54 is -19, or 35. Note that $-19 \equiv 35$ 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 $2x + y \equiv 4 \pmod{7}$.

Solution:

(a) Multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get $x \equiv 5 \pmod{11}$.

(b) Subtract 15 from both sides to get $3x \equiv 10 \pmod{21}$. Now note that this implies $3x \equiv 1 \pmod{3}$, since 3 divides 21, and the latter equation has no solution, so the former cannot either.

We are using the fact that if $d \mid m$, then $x \equiv y \pmod{m}$ implies $x \equiv y \pmod{d}$ (but not necessarily the other way around). To see this, if $x \equiv y \pmod{m}$, then $m \mid x - y$ (by definition) and so $d \mid x - y$, and hence $x \equiv y \pmod{d}$.

(c) First, subtract the first equation from double the second equation to get $2(2x + y) - (3x + 2y) \equiv x \equiv 1 \pmod{7}$; now plug in to the second equation to get $2 + y \equiv 4 \pmod{7}$, so the system has the solution $x \equiv 1 \pmod{7}$, $y \equiv 2 \pmod{7}$.