CS 70 Discrete Mathematics and Probability Theory
Spring 2018 Satish Rao and Babak Ayazifar

DIS 3A

1 Modular Potpourri

(a) Evaluate $4^{96} \pmod 5$.

(b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod 6$.

(c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

Solution:

(a) One way: $4 \equiv -1 \pmod 5$, and $(-1)^{96} \equiv 1$.

Another: $4^2 \equiv 1 \pmod 5$, so $4^{96} = (4^2)^{48} \equiv 1 \pmod 5$.

Mention that it is **invalid** to "apply the mod to the exponent": $4^{96} \not\equiv 4^1 \pmod 5$.

(b) Impossible.

Suppose there exists an x satisfying both equations.

From $x \equiv 3 \pmod{16}$, we have $x = 3 + 16k$ for some integer k. This implies $x \equiv 1 \pmod 2$.

From $x \equiv 4 \pmod 6$, we have $x = 4 + 6l$ for some integer l. This implies $x \equiv 0 \pmod 2$.

Now we have $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 2$. Contradiction.

(c) False, consider $x \equiv 8 \pmod{12}$.

The reason we can't eliminate the 2 in the first equation to get the second equation is because 2 does not have a multiplicative inverse modulo 12, as 2 and 12 are not coprime.

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

In this problem we will consider the 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:

$$\begin{aligned}
\gcd(2328, 440) &= \gcd(440, 128) && [\mathbf{128} = 1 \times \mathbf{2328} + (-5) \times \mathbf{440}] \\
&= \gcd(128, 56) && [\mathbf{56} = 1 \times \mathbf{440} + ____ \times \mathbf{128}] \\
&= \gcd(56, 16) && [\mathbf{16} = 1 \times \mathbf{128} + ____ \times \mathbf{56}] \\
&= \gcd(16, 8) && [\mathbf{8} = 1 \times \mathbf{56} + ____ \times \mathbf{16}] \\
&= \gcd(8, 0) && [\mathbf{0} = 1 \times \mathbf{16} + (-2) \times \mathbf{8}] \\
&= 8.
\end{aligned}$$

(Fill in the blanks)

(b) Now working back up from the bottom, we will express the final gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned}
8 &= 1 \times \mathbf{8} + 0 \times \mathbf{0} = 1 \times \mathbf{8} + (1 \times \mathbf{16} + (-2) \times \mathbf{8}) \\
&= 1 \times \mathbf{16} - 1 \times \mathbf{8} \\
&= ____ \times \mathbf{56} + ____ \times \mathbf{16}
\end{aligned}$$

[*Hint*: Remember, $\mathbf{8} = 1 \times \mathbf{56} + (-3) \times \mathbf{16}$. Substitute this into the above line.]

$$= \_\_\_\_ \times \mathbf{128} + \_\_\_\_ \times \mathbf{56}$$

[*Hint*: Remember, $\mathbf{16} = 1 \times \mathbf{128} + (-2) \times \mathbf{56}$.]

$$= \_\_\_\_ \times \mathbf{440} + \_\_\_\_ \times \mathbf{128}$$
$$= \_\_\_\_ \times \mathbf{2328} + \_\_\_\_ \times \mathbf{440}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

Solution:

(a) -3

-2

-3

(b) $1 \times \mathbf{16} - 1 \times (1 \times \mathbf{56} + (-3) \times \mathbf{16}) = -1 \times \mathbf{56} + 4 \times \mathbf{16}$

$-1 \times \mathbf{56} + 4 \times (1 \times \mathbf{128} + (-2) \times \mathbf{56}) = 4 \times \mathbf{128} - 9 \times \mathbf{56}$

$4 \times \mathbf{128} - 9 \times (1 \times \mathbf{440} + (-3) \times \mathbf{128}) = -9 \times \mathbf{440} + 31 \times \mathbf{128}$

$-9 \times \mathbf{440} + 31 \times (1 \times \mathbf{2328} + (-5) \times \mathbf{440}) = 31 \times \mathbf{2328} - 164 \times \mathbf{440}$

(c) $\gcd(17, 38) = 1 = 13 \times 38 - 29 \times 17$; also, more simply, $-4 \times 38 + 9 \times 17$, but the algorithm produces the former.

(d) It is equal to -29, which is equal to 9.