CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

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}.

(c) Find the last digit of 3^{641}.

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

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

(c) Notice that $3^4 = 9^2$ so using that $9^2 \equiv 1 \pmod{10}$ (since 9 is its own multiplicative inverse mod 10), we have $3^4 \equiv 1 \pmod{10}$. We also have that $641 = 160 \cdot 4 + 1$, so

$$3^{641} \equiv 3^{4(160)} \cdot 3 \equiv 1^{160} \cdot 3 \equiv 3 \pmod{10},$$

making the last digit a 3.

2 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: $2x \equiv 4 \mod 12 \iff x \equiv 2 \pmod{12}$.

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": $4^{96} \neq 4^1 \pmod 5$

(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.

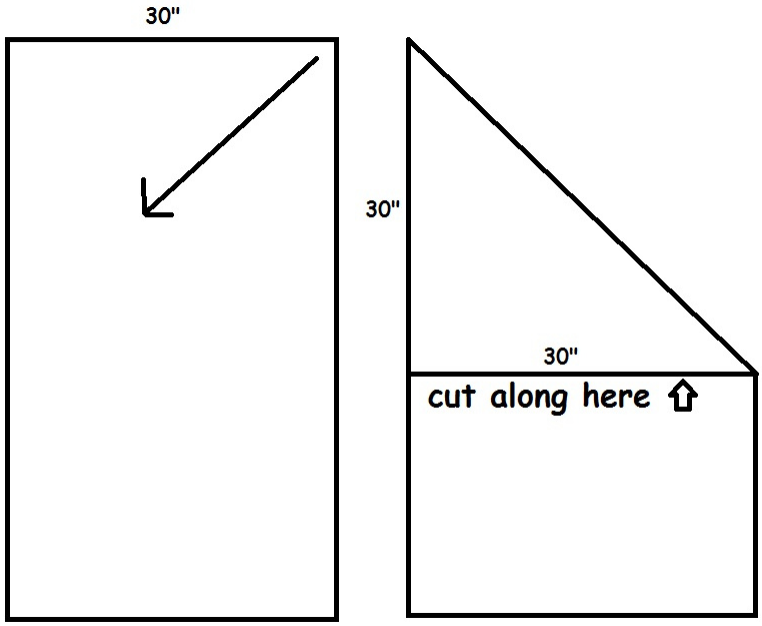
(c) False, consider $x \equiv 8$.

3 Paper GCD

Given a sheet of paper such as this one, and no rulers, describe a method to find the GCD of the width and the height of the paper. You can fold or tear the paper however you want, and ultimately you should produce a square piece whose side lengths are equal to the GCD.

Solution:

We can fold the smaller side diagonally onto the larger side, and tear the paper from where the fold lands.



If we started with height and width equal to a and b, this gives us a piece of paper with side lengths $a-b$ and b (assuming that $a > b$). Note that if $a-b > b$, the next time we end up with side lengths $a-2b$ and b. So after a few steps we must reach $a \pmod{b}$ and b, at which we start subtracting from b.

Continuing this method is similar to the Euclidean algorithm and therefore results in reaching 0 at some point. Right before reaching 0, we must have a square piece of paper whose side lengths are the GCD.

4 Extended Euclid

In this problem we will consider the extended Euclid's algorithm.

1. Calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.
2. What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?
3. 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:

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

(Fill in the blanks.)

4. 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:

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

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

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

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

$$\begin{aligned}
&= ____ \times \mathbf{440} + ____ \times \mathbf{128} \\
&= ____ \times \mathbf{2328} + ____ \times \mathbf{440}
\end{aligned}$$

Solution:

1. First, we compute their GCD.

$$\begin{aligned}
\gcd(38,17) &= \gcd(17,4) && [\mathbf{4} = \mathbf{38} - 2 \times \mathbf{17}] \\
&= \gcd(4,1) && [\mathbf{1} = \mathbf{17} - 4 \times \mathbf{4}] \\
&= \gcd(1,0) && [\mathbf{0} = \mathbf{4} - 4 \times \mathbf{1}] \\
&= 1
\end{aligned}$$

Then, we work from bottom.

$$\begin{aligned}
1 &= 1 \times \mathbf{1} + \mathbf{0} \\
&= 1 \times \mathbf{1} + (\mathbf{4} - 4 \times \mathbf{1}) \\
&= \mathbf{4} - 3 \times \mathbf{1} = \mathbf{4} - 3 \times (\mathbf{17} - 4 \times \mathbf{4}) \\
&= -3 \times \mathbf{17} + 13 \times \mathbf{4} = -3 \times \mathbf{17} + 13 \times (\mathbf{38} - 2 \times \mathbf{17}) \\
&= 13 \times \mathbf{38} - 29 \times \mathbf{17}
\end{aligned}$$

Thus, we have $\gcd(17,38) = 1 = 13 \times 38 - 29 \times 17$.

2. It is equal to -29, which is equal to 9.

3. 3

   2

   3

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

   $4 \times \mathbf{128} - 9 \times \mathbf{56}$

   $-9 \times \mathbf{440} + 31 \times \mathbf{128}$

   $31 \times \mathbf{2328} - 164 \times \mathbf{440}$