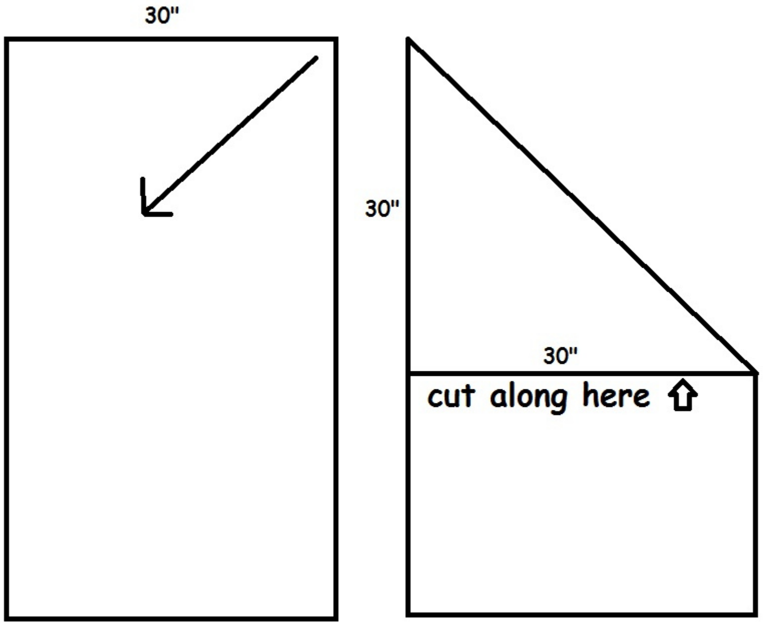
CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand

Discussion 4B

1. **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.

2. **Baby Fermat**

Assume that a does have a multiplicative inverse $\pmod{m}$. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

Solution: There are only m possible values $\pmod{m}$, and so after the m-th term we should see repetitions.

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

Solution: If we multiply both sides by $(a^*)^j$, where a^* is the multiplicative inverse, we get $a^{i-j} \equiv 1 \pmod{m}$.

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution: We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod{m}$.

3. **Party Tricks** You are at a party celebrating your completion of the CS70 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}.

Solution: 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) Find the last digit of 9^{9999}.

Solution: 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) Find the last digit of 3^{641}.

Solution: 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.

4. **Extended Euclid**

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

(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:

$gcd(2328,440)$
$= gcd(440,128)$ $[128 \equiv 2328 \bmod 440 \equiv 2328 - 5 \times 440]$
$= gcd(128,56)$ $[56 \equiv 440 \bmod 128 \equiv 440 - \_\_\_\_ \times 128]$ **Solution:** 3
$= gcd(56,16)$ $[16 \equiv 128 \bmod 56 \equiv 128 - \_\_\_\_ \times 56]$ **Solution:** 2
$= gcd(16,8)$ $[8 \equiv 56 \bmod 16 \equiv 56 - \_\_\_\_ \times 16]$ **Solution:** 3
$= gcd(8,0)$ $[0 \equiv 16 \bmod 8 \equiv 16 - 2 \times 8]$
$= 8.$
(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:

8
$= 1 \times 8 + 0 \times 0 = 1 \times 8 + (16 - 2 \times 8)$
$= 1 \times 16 - 1 \times 8$
$= \_\_\_\_ \times 56 + \_\_\_\_ \times 16$ [Hint: Remember, $8 = 56 - 3 \times 16$. Substitute this into the above line...]
Solution: $1 \times 16 - 1 \times (56 - 3 \times 16) = -1 \times 56 + 4 \times 16$

$= \_\_\_\_ \times 128 + \_\_\_\_ \times 56$ [Hint: Remember, $16 = 128 - 2 \times 56$]
Solution: $4 \times 128 - 9 \times 56$

$= \_\_\_\_ \times 440 + \_\_\_\_ \times 128$
Solution: $-9 \times 440 + 31 \times 128$

$= \_\_\_\_ \times 2328 + \_\_\_\_ \times 440$
Solution: $31 \times 2328 - 164 \times 440$

(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.

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

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

Solution: It is equal to -29, which is equal to 9.

5. **Combining moduli**

Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5,8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod 5$ and $c \pmod 8$.

(a) What is $8 \pmod 5$ and $8 \pmod 8$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod 5$ and $a \equiv 0 \pmod 8$.
Solution: $8 \equiv 3 (\text{mod } 5)$ and $8 \equiv 0 (\text{mod } 8)$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 (\text{mod } 5)$. Therefore 16 satisfies both conditions.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod 5$ and $b \equiv 1 \pmod 8$.
Solution: We can find such a number by considering multiples of 5,i.e.0,5,10,15,20,25,30,35, and find that if $b = 25$, $25 \equiv 1 (\text{mod } 8)$, so it satisfies both conditions.

(c) Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod 5$ and $c \equiv 5 \pmod 8$. Find c by expressing it in terms of a and b.
Solution: We claim $c \equiv 2a + 5b \equiv 37 (\text{mod } 40)$. To see that $c \equiv 2 (\text{mod } 5)$, we note that $b \equiv 0 (\text{mod } 5)$ and $a \equiv 1 (\text{mod } 5)$. So $c \equiv 2a \equiv 2 (\text{mod } 5)$. Similarly $c \equiv 5b \equiv 5 (\text{mod } 8)$.

(d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod 5$ and $d \equiv 4 \pmod 8$.
Solution: We can repeat the same procedure as above, and find that $d = 3a + 4b \equiv 28 (\text{mod } 40)$.

(e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod 5$, and $c \times d \equiv 5 \times 4 \pmod 8$?
Solution: $c \times d = 37 \times 28 \equiv 36$ (mod 40). Note that if $a \equiv b$ (mod n) and $c \equiv d$ (mod n) then $a \times c \equiv b \times d$ (mod n).Therefore we can multiply $c \equiv 2$ (mod 5) and $d \equiv 3$ (mod 5) to get $c \times d \equiv 2 \times 3$ (mod 5). Similarly we can multiply these equations (mod 8) and get $c \times d = 5 \times 4$ (mod 8).