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.

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 $a, a^2, a^3, \dots \pmod{m}$. Prove that this sequence has repetitions.

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

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

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}.

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

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

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:
   $gcd(2328, 440)$
   $= gcd(440, 128)$ $[128 \equiv 2328 \bmod 440 \equiv 2328 - 5 \times 440]$
   $= gcd(128, 56)$ $[56 \equiv 440 \bmod 128 \equiv 440 - \underline{\quad\quad} \times 128]$
   $= gcd(56, 16)$ $[16 \equiv 128 \bmod 56 \equiv 128 - \underline{\quad\quad} \times 56]$
   $= gcd(16, 8)$ $[8 \equiv 56 \bmod 16 \equiv 56 - \underline{\quad\quad} \times 16]$
   $= gcd(8, 0)$ $[0 \equiv 16 \bmod 8 \equiv 16 - 2 \times 8]$
   $= 8.$
   (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...]

$=$ ____ $\times 128 +$ ____ $\times 56$ [Hint: Remember, $16 = 128 - 2 \times 56$]

$=$ ____ $\times 440 +$ ____ $\times 128$

$=$ ____ $\times 2328 +$ ____ $\times 440$

(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.

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

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 $a \equiv 0 \pmod 8$.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod 5$ and $b \equiv 1 \pmod 8$.

(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.

(d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod 5$ and $d \equiv 4 \pmod 8$.

(e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod 5$, and $c \times d \equiv 5 \times 4 \pmod 8$?