EECS 70 Discrete Mathematics and Probability Theory
Fall 2015 Satish Rao

Discussion 4B

1. **Recursive Calls** Calculate the greatest common divisor (gcd) of the following pairs of numbers using the Euclidean algorithm.

   [Hasty refresher: starting with a pair of input values, keep repeating the operation "Replace the larger value with its remainder modulo the smaller value" over and over, until one of the values becomes zero. At that point, the other value is the gcd of the original two inputs (as well as of every pair of values along the way). In pseudocode: gcd$(x,y) \rightarrow$ if $y = 0$ then return x else return gcd$(y, x \mod y)$].

   1. 208 and 872
   2. 1952 and 872
   3. $1952 \times n + 872$ and 1952

   Solution: **Motivation for Problem:** This is supposed to be a quick refresher for the gcd algorithm, and attempts to show how gcd creates recursive calls of other gcd that we can use to shortcut.

   Solutions: 8 for all of these. The first answer students should calculate by hand, the second answer will reduce to the first after one step, and the third answer will reduce to the second in one step.

2. **Amaze your friends!**

   1. You want to trick your friends into thinking you can perform mental arithmetic with very large numbers What are the last digits of the following numbers?

      i. 11^{2014}

      ii. 9^{10001}

      iii. $3^{987654321}$

   2. You know that you can quickly tell a number n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. Prove that you can use this trick to quickly calculate if a number is divisible by 9.

   Solution: **Motivation for Problem:** This problem causes students to start recognizing tricks regarding modular arithmetic. This lays the ground later for proving properties of modular arithmetic.

   Solutions:

   1. i. 11 is always 1 mod 10 therefore the answer to (a) is 1.

      ii. 9 is its own inverse mod 10, therefore, if 9 is raised to an odd power, the number will be 9 mod 10. So the answer is 9

      iii. $3^4 = 9^2 = 1 \mod 10$. We see that the exponent $987654321 = 1 \mod 4$ so the answer is 3.

   2. Let n be written as $a_k a_{k-1} \cdots a_1 a_0$ where the a_i are digits, base-10. We can write
      $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10 a_1 + a_0 = (10^k - 1) a_k + (10^{k-1} - 1) a_{k-1} + \cdots + (10-1) a_1 + \sum_{i=0}^{k} a_i$
      The first few terms are all divisible 9; they're all of the form $99 \cdots 99 \cdot a_i$. So if the sum at the end is divisible by 9, then n is too and vice versa.

3. **Product of Two**

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > \frac{p}{2}$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.

Solution: Given x, consider the set T defined as $\{xy^{-1} \pmod{p} : y \in S\}$. Note that the set T has the same cardinality as S, because for $y_1 \neq y_2 \pmod{p}$, we have $xy_1^{-1} \neq xy_2^{-1} \pmod{p}$ (if not, we can multiply both sides by x^{-1}, and take the inverse to get a contradiction).

Therefore the set S and T must have a nonempty intersection. So there must be $y_1, y_2 \in S$ such that $xy_1^{-1} = y_2 \pmod{p}$. But this means that $x = y_1 y_2 \pmod{p}$.

4. **Extended Euclid**

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

1. 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:
   $gcd(2328, 440)$
   $= gcd(440, 128)$ [$128 \equiv 2328 \bmod 440 \equiv 2328 - 5 \times 440$]
   $= gcd(128, 56)$ [$56 \equiv 440 \bmod 128 \equiv 440 -$ ____ $\times 128$] **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)

2. 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: $31 \times 2328 - 164 \times 440$

3. 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.

4. 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.