CS 70 Discrete Mathematics and Probability Theory
Spring 2016 Rao and Walrand Discussion 4A

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: 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. Answer: 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. 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 $k \geq 0$.

- 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.
- 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 $a^{i-j} \equiv 1 \pmod m$.
- 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. 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:
   $gcd(2328, 440)$
   $= gcd(440, 128)$ [$128 \equiv 2328 \bmod 440 \equiv 2328 - 5 \times 440$]
   $= gcd(128, 56)$ [$56 \equiv 440 \bmod 128 \equiv 440 - \_\_\_\_ \times 128$]
   $= gcd(56, 16)$ [$16 \equiv 128 \bmod 56 \equiv 128 - \_\_\_\_ \times 56$]
   $= gcd(16, 8)$ [$8 \equiv 56 \bmod 16 \equiv 56 - \_\_\_\_ \times 16$]
   $= gcd(8, 0)$ [$0 \equiv 16 \bmod 8 \equiv 16 - 2 \times 8$]
   $= 8$.
   (Fill in the blanks)
   Solution: 3, 2, 3
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...]

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

   $= \_\_\_\_ \times 440 + \_\_\_\_ \times 128$

   $= \_\_\_\_ \times 2328 + \_\_\_\_ \times 440$

   Solution:
   $1 \times 16 - 1 \times (56 - 3 \times 16) = -1 \times 56 + 4 \times 16$,
   $4 \times 128 - 9 \times 56$,
   $-9 \times 440 + 31 \times 128$,
   $31 \times 2328 - 164 \times 440$
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.