EECS 70 Discrete Mathematics and Probability Theory
Spring 2014 Anant Sahai

Discussion 4B

1. **Amaze your friends!**

   (a) 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. $3^{987654321}$

   (b) 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.

2. **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 $\gcd(y, x \mod y)$].

   (a) 208 and 872

   (b) 1952 and 872

   (c) $1952 \times n + 872$ and 1952

3. **Extend it!**

   In this problem we will consider extending the gcd algorithm.

   (a) 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 ?)

   (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?

4. **Practicing Extensions** Here is a refresher of the extended gcd algorithm:

```
algorithm extended-gcd(x,y)
  if y = 0 then return(x, 1, 0)
  else
    (d, a, b) := extended-gcd(y, x mod y)
    return((d, b, a - (x div y) * b))
```

   Using this, find the inverse of 26 mod 35.

5. Prove that $\gcd(7n+4, 5n+3) = 1$ for all $n \in \mathbb{N}$.