# Homework 3

Discrete Structures
CS 173 [B] : Fall 2012

Released: Tue Sep 18
Due: Wed Sep 26, 3:00 PM

1. **Euclidean Algorithm** [15 point]

   (a) Trace the execution of the Euclidean algorithm on the inputs $a = 837$ and $b = 2015$. That is, give a table showing the values of the main variables ($x$, $y$, $r$, in the description in the textbook) for each pass through the loop. Explicitly indicate what the output value is.

   (b) **Speed of Euclidean Algorithm.** The Euclidean algorithm zooms into the answer quite quickly. This is because, at each step one of the numbers is replaced by a number which is at most half of it. To see this, prove the following.

   If $x, y$ are positive integers with $y \leq x$, and $r$ is the remainder on dividing $x$ by $y$ (i.e., $x \equiv r \pmod{y}$ and $0 \leq r < y$), then $r < \frac{x}{2}$.

   [Hint: consider two cases: $y \leq \frac{x}{2}$ and $y > \frac{x}{2}$. In the latter case, what is $r$?]

2. **Congruence mod $m$.** [25 points]

   Recall the following definition: integers $a$ and $b$ are congruent modulo an integer $m$ (in shorthand: $a \equiv b \pmod{m}$) if and only if there is an integer $k$ such that $a = b + km$. Prove the following statements directly using the above definition, together with high school algebra. Do not use other facts about modular arithmetic proved in class or in the book. You may use part (a) in part (b). Make sure your steps are in logical order.

   (a) For any integers $p$, $q$, $s$, $t$ and $m$, If $p \equiv q \pmod{m}$ and $s \equiv t \pmod{m}$, then $ps \equiv qt \pmod{m}$.

   (b) For all integers $a$, $b$, $c$, $d$ and any even integer $m$, if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $3ab + bd - \frac{m}{2} \equiv 3cd + d^2 + \frac{m}{2} \pmod{m}$.

3. **Prime numbers.** [15 points]

   Prove that if $p$ is a prime number such that $p \equiv 1 \pmod{3}$, then $p \equiv 1 \pmod{6}$.

   [Hint: What can you say about the quotient when dividing $p$ by 3? Alternately, can you argue that $p \not\equiv 4 \pmod{6}$? (And then what?)]

4. **Congruence mod $m$ and GCD.** [20 points]

   Show that if $x$, $y$ and $m$ are integers such that $x \equiv y \pmod{m}$, then $gcd(x, m) = gcd(y, m)$.

   [Hint: What would the Euclidean algorithm do? (But your proof should work not only for positive integers.)]

5. **A Set representing Prime Factorization.** [25 points]

   For every positive integer $n$, define a set $PF_n \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ to denote the prime factors of $n$, as follows.

   $$PF_n = \{(p, i) : p \text{ is prime, } i \in \mathbb{Z}^+ \text{ and } (p^i \mid n)\}.$$

(a) What is $PF_1$?

(b) Explicitly write down $PF_{12}$ and $PF_{30}$.

(c) Write down $PF_{\gcd(12,30)}$.

(d) Write down $PF_{\mathrm{lcm}(12,30)}$.

(e) For any two positive integers $m$ and $n$, give formulas for $PF_{\gcd(m,n)}$ and $PF_{\mathrm{lcm}(m,n)}$ in terms of $PF_m$ and $PF_n$.