Homework 2

Discrete Structures
CS 173 [B] : Fall 2015

Released: Fri Feb 13
Due: Fri Feb 20, 10:00 PM

Submit on Moodle.

1. **Euclidean Algorithm** [25 points]

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

   Then, find two integers u, v such that $837u + 2015v = \gcd(837, 2015)$.

   [Hint: For the second part, you'll have to work backwards through the table. It will be helpful to maintain another column in your table for the quotient, q, so that $r = x - qy$. Find the first time the gcd appears as a remainder r, and write it as $x - qy$. Now, moving to the previous step, write this is an expression in terms of y and r. Iteratively, replace r similarly, maintaining an expression of the form $\alpha x + \beta y$ at each row.]

   (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. **Lattice.** [25 points]

   Over $\mathbb{Z} \times \mathbb{Z}^+ \times \mathbb{Z}^+$, define the predicate $M(x, a, b)$ to be true iff $\gcd(a, b) \mid x$ (i.e., x is a multiple of $\gcd(a, b)$). Also define the predicate $L(x, a, b)$ to be true iff $\exists r, s \in \mathbb{Z}\ \ x = ra + sb$. (This says that x is in the "lattice" generarted by a and b.) Prove that

   $$\forall x \in \mathbb{Z}, \forall a, b \in \mathbb{Z}^+\ M(x, a, b) \leftrightarrow L(x, a, b).$$

   [Hint: You will have to show both $L(x, a, b) \rightarrow M(x, a, b)$ and $M(x, a, b) \rightarrow L(x, a, b)$. The first one you should be able to show from the definitions. For the other direction, you can use the fact (implied by the Euclidean algorithm for GCD) that $\forall p, q \in \mathbb{Z}^+\ \exists u, v \in \mathbb{Z}\ \ \gcd(p, q) = up + vq$.]

3. **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.

(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 any integers x, y and m, if $x \equiv y \pmod{m}$, then $\gcd(x, m) = \gcd(y, m)$.

[Hint: Show that, in fact, not just the gcd, but all common factors of (x, m) are common factors of (y, m), and vice versa.]

4. **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.