Homework 2

Discrete Structures
CS 173 [B] : Fall 2015

February 17, 2015

Solutions for Manually Graded Problems.

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.]

   Solution:

   Solution: Below, $r = \text{remainder}(x, y)$ is the remainder on dividing x by y, $q = \text{quotient}(x, y)$ is quotient.

x	y	r	q	$r = x - q \cdot y$
2015	837	341	2	$341 = 2015 - 2 \cdot 837$
837	341	155	2	$155 = 837 - 2 \cdot 341$
341	155	31	2	$31 = 341 - 2 \cdot 155$
155	31	0	5	

   Hence, we have $\gcd(2015, 837) = 31$. Also, from this table we can write:

$$\begin{aligned} 31 &= 341 - 2 \times 155 \\ &= 341 - 2 \times (837 - 2 \times 341) = 5 \times 341 - 2 \times 837 \\ &= 5 \times (2015 - 2 \times 837) - 2 \times 837 = 5 \times 2015 - 12 \times 837 \end{aligned}$$

   Thus we have $837u + 2015v = 31$ for $u = -12$ and $v = 5$.

   (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?]

Solution:

Since r is the remainder when x is divided by y, we have $r < y$. So, if $y \leq x$, then we get $r < \frac{x}{2}$. If $y > x/2$, then $r = x - y$ (quotient is 1), and again $r < \frac{x}{2}$.

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 $L(x, a, b) \to M(x, a, b)$ and $M(x, a, b) \to L(x, a, b)$. 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 $\forall p, q \in \mathbb{Z}^+ \; \exists u, v \in \mathbb{Z} \;\; \gcd(p, q) = up + vq$.]

Solution:

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

Suppose x is an arbitrary integer and a, b are arbitrary positive integers. We will show that $L(x, a, b) \to M(x, a, b)$ and $M(x, a, b) \to L(x, a, b)$.

<u>$L(x, a, b) \to M(x, a, b)$:</u> Suppose $L(x, a, b)$ holds. That is, $\exists r, x \in \mathbb{Z} \;\; x = ra + sb$. Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$ (since, by definition of gcd, it is a divisor of both the numbers). So there exist integers t_1, t_2 such that $a = t_1 d$ and $b = t_2 d$. Hence, $x = r(t_1 d) + s(t_2 d) = (rt_1 + st_2)d$. Thus, $d|x$ or in other words $\gcd(a, b)|x$. Thus, by definition, $M(x, a, b)$ holds.

<u>$L(x, a, b) \to M(x, a, b)$:</u> Suppose $M(x, a, b)$ holds. That is, $\gcd(a, b)|x$. So there exists an integer t such that $x = t \gcd(a, b)$. Since $a, b \in \mathbb{Z}^+$, by the hint, there exist integers u, v such that $\gcd(a, b) = ua + vb$. So $x = t(ua + vb) = (tu)a + (tv)b$. Since u, v, t are integers, so are tu and tv. Thus, $x = ra + sb$, where $r = tu$ and $s = tv$ are integers. Thus by definition of L, $L(x, a, b)$ holds.

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 $ps \equiv qt \pmod{m}$.

Solution: Let p, q, s, t and m be integers such that $p \equiv q \pmod{m}$ and $s \equiv t \pmod{m}$. Then, by the definition of congruence mod m, there exist integers k, ℓ such that $p = q + km$ and $s = t + \ell m$. Then,

$$ps - qt = (q + km)(t + \ell m) - qt = kmt + q\ell m + k\ell m^2 = wm,$$

where $w = kt + \ell q + k\ell m$. That is $(ps - qt)|m$, or equivalently, $ps \equiv qt \pmod{m}$.

(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.]

Solution: Since $x \equiv y \pmod{m}$ we have $x = km + y$ for some integer k. Suppose d is a common divisor of x and m (**not** necessarily the greatest common divisor). Then $d|km + y$ and $d|m$. That is, $\alpha d = (km + y)$ and $\beta d = m$ for integers α, β. Hence, $y = \alpha d - km = \alpha d - k\beta d = d(\alpha - \beta k)$. Hence $d|y$. In other words, any common divisor of x and y is a common divisor of y and m.

Identical reasoning shows that any common divisor of y and m is a common divisor of x and m. Therefore, the set of common divisors of x and m is the same as the set of common divisors of y and m, which in particular means that they share the greatest common divisor.

Alternate solution

By definition, $x = km + y$ for some integer k. Let $d = \gcd(x, m)$. By definition, $d|x$, which implies that $d|km + y$. Since d also divides m, we note that $d|y$ (as in the above solution). Now suppose there is some larger d' such that $d'|y$ and $d'|m$. However, since $y = x - km$, this would imply that $d'|x$ as well, contradicting the fact that d is the GCD of x and m.

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?

Solution: $PF_1 = \emptyset$ (since 1 has no prime factors).

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

Solution: $PF_{12} = \{(2, 1), (2, 2), (3, 1)\}$.
$PF_{30} = \{(2, 1), (3, 1), (5, 1)\}$.

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

Solution: $\gcd(12, 30) = 6$. $PF_6 = \{(2, 1), (3, 1)\}$.

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

Solution: $\text{lcm}(12, 30) = 60$. $PF_{60} = \{(2, 1), (2, 2), (3, 1), (5, 1)\}$.

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

Solution: $PF_{\gcd(m,n)} = PF_m \cap PF_n$ and $PF_{\text{lcm}(m,n)} = PF_m \cup PF_n$.