CPSC 513 — Assignment #1

Solutions for Question #1

Recall that if n and m are nonnegative integers then the ***least common multiple*** of n and m, lcm(n, m), is (usually) the smallest positive integer that is divisible by both n and m.

- There is a special case: For every integer $k \in \mathbb{N}$, lcm$(k, 0) =$ lcm$(0, k) = k$ — so that lcm$(0, 0) = 0$.
- If $k \geq 1$ then lcm$(k, 1) =$ lcm$(1, k) = k$ as well.

The ***greatest common divisor*** of n and m, $\gcd(n, m)$, is the largest integer that divides both n and m.

- There is an exception: $\gcd(0, 0)$ will be defined to be 0.
- If $k \geq 1$ then $\gcd(k, 0) = \gcd(0, k) = k$ — and this follows by the above definition of $\gcd(n, m)$.
- If $k \geq 1$ then $\gcd(k, 1) = \gcd(1, k) = 1$.

A bit more information will be helpful when $n, m \geq 2$. Recall that every positive integer that is greater than or equal to two has a ***factorization*** as a ***product of primes*** — so that if $n, m \geq 2$ then there exists an integer $k \geq 1$, a set of *distinct* primes

$$p_1, p_2, \ldots, p_k,$$

and *unique* nonnegative integers $e_1, e_2, \ldots, e_k$ and $f_1, f_2, \ldots, f_k$ such that

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

and

$$m = p_1^{f_1} \times p_2^{f_2} \times \cdots \times p_k^{f_k}.$$

(a) You were first asked to identify the factorizations of lcm(n, m) and $\gcd(n, m)$.

Solution: When $n, m \geq 2$ and have factorizations as given above, then

$$\text{lcm}(n, m) = p_1^{\max(e_1, f_1)} \times p_2^{\max(e_2, f_2)} \times \cdots \times p_k^{\max(e_k, f_k)}$$

and

$$\gcd(n, m) = p_1^{\min(e_1, f_1)} \times p_2^{\min(e_2, f_2)} \times \cdots \times p_k^{\min(e_k, f_k)}.$$

(b) You were next asked how large lcm(n, m) can be.

Solution: Since $\max(e_i, f_i) \leq e_i + f_i$ for $1 \leq i \leq k$ it follows by the above that if $n, m \geq 2$ then

$$\text{lcm}(n, m) \leq n \times m.$$

Indeed, this bound is "tight:" If n and m have no common factors then lcm$(n, m) = n \times m$. Furthermore, it follows by the definitions given above for lcm$(1, m)$ and lcm$(n, 1)$ that the above inequality is also satisfied when $n, m \geq 1$.

(c) You were asked what the answer for (a) implies about the relationship between lcm(n, m) and $\gcd(n, m)$.

Solution: Since $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$, for $1 \leq i \leq k$, it follow by the answer for (a) that if $n, m \geq 2$ then

$$\text{lcm}(n, m) \times \gcd(n, m) = n \times m.$$

Indeed, it follows by the definition of lcm$(1, m)$, lcm$(n, 1)$, $\gcd(1, m)$ and $\gcd(n, 1)$, given above, that the above equation holds whenever $n, m \geq 1$.

(d) Finally, you were asked to use the above information to prove that the functions lcm(n, m) and $\gcd(n, m)$ are both primitive recursive.

Solution: Let us begin by considering the predicate $p : \mathbb{N}^3 \to \{0, 1\}$ such that, for all $x_1, x_2, t \in \mathbb{N}$,

$$p(x_1, x_2, t) = \begin{cases} 1 & \text{if } (t = 0 \bmod x_1) \wedge (t = 0 \bmod x_2) \wedge \neg(t = 0) \\ 0 & \text{otherwise.} \end{cases}$$

Since the "mod" function is primitive recursive, testing equality of natural numbers is primitive recursive, and the conjunction (or "and") and negation of primitive recursive predicates is primitive recursive, this is certainly a primitive recursive predicate.

Note as well that if $x_1, x_2 \geq 1$ then, for $t \in \mathbb{N}$, $p(x_1, x_2, t) = 1$ if and only if $t > 0$ and t is a multiple of both x_1 and x_2.

Let $g : \mathbb{N}^3 \to \mathbb{N}$ be the function such that, for all $x_1, x_2, y \in \mathbb{N}$,

$$g(x_1, x_2, y) = \min_{t \leq y} p(x_1, x_2, t).$$

This is certainly a primitive recursive function — because it is has been obtained from a primitive recursive predicate using ***bound minimization***. It should not be hard to see that when $x_1, x_2, y \geq 1$,

$$g(x_1, x_2, y) = \begin{cases} \mathsf{lcm}(x_1, x_2) & \text{if } y \geq \mathsf{lcm}(x_1, x_2), \\ 0 & \text{otherwise.} \end{cases}$$

Let $h : \mathbb{N}^2 \to \mathbb{N}$ such that, for all $x_1, x_2 \in \mathbb{N}$,

$$h(x_1, x_2) = g(x_1, x_2, x_1 \times x_2).$$

Since the multiplication function (of a pair of natural numbers) is primitive recursive it should not be hard to see that h is primitive recursive — because it is obtained from multiplication, the above function g, and the initial functions using composition. Notice as well that — by the result of part (b), above,

$$h(x_1, x_2) = \mathsf{lcm}(x_1, x_2)$$

whenever $x_1, x_2 \geq 1$.

Notice that if $x_1 = 0$ or $x_2 = 0$ then

$$\mathsf{lcm}(x_1, x_2) = x_1 + x_2,$$

and the addition function of two natural numbers is primitive recursive. Finally, notice that the predicate $q : \mathbb{N}^2 \to \{0, 1\}$ such that, for all $x_1, x_2 \in \mathbb{N}$,

$$q(x_1, x_2) = \begin{cases} 1 & \text{if } (x_1 = 0) \vee (x_2 = 0) \\ 0 & \text{otherwise} \end{cases}$$

is also a primitive recursive predicate — this is the disjunction (or "or") of the primitive recursive predicates testing equality of each of x_1 and x_2 with 0.

Thus the function $\mathsf{lcm}(x_1, x_2)$ of x_1 and x_2 can now be seen to be primitive recursive, because

$$\mathsf{lcm}(x_1, x_2) = \begin{cases} x_1 + x_2 & \text{if } q(x_1, x_2) = 1, \\ h(x_2, x_2) & \text{otherwise.} \end{cases}$$

— that is, it can be constructed from a pair of primitive recursive functions and a primitive recursive predicate using ***definition by cases***.

It now follows (almost immediately) that $\gcd(x_1, x_2)$ is a primitive recursive function of x_1 and x_2 as well — because, for all $x_1, x_2 \in \mathbb{N}$,

$$\gcd(x_1, x_2) = \begin{cases} x_1 + x_2 & \text{if } q(x_1, x_2) = 1, \\ (x_1 \times x_2) \text{ quo } \mathsf{lcm}(x_1, x_2) & \text{otherwise.} \end{cases}$$

— and multiplication and the "division with remainder function" quo have already been shown to be primitive recursive — so that the function of x_1 and x_2,

$$(x_1 \times x_2) \text{ quo } \mathsf{lcm}(x_1, x_2)$$

is now easily seen to be primitive recursive as well.