MA 261 Homework 6 - Solutions

1. (i) Find all solutions to the linear Diophantine equation

$$7x + 10y = 1$$

Proof. Applying the Euclidean algorithm, we have

$$\begin{aligned} 10 &= 7(1) + 3 \\ 7 &= 3(2) + 1 \\ 3 &= 1(3) + 0 \end{aligned}$$

Thus

$$1 = 7 - 3(2) = 7 - (10 - 7(1))(2) = 7(3) + 10(-2),$$

so we have an initial solution $x_0 = 3$, $y_0 = -2$. Then by Theorem 1.53, all solutions are of the form

$$x = 3 + 10k, \quad y = -2 - 7k.$$

□

(ii) Find all solutions to the linear Diophantine equation

$$6x + 15y = 3$$

Proof. Applying the Euclidean algorithm, we have

$$\begin{aligned} 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0 \end{aligned}$$

Thus

$$3 = 6(-2) + 15(1)$$

so we have an initial solution $x_0 = -2$, $y_0 = 1$. Then by Theorem 1.53, all solutions are of the form

$$x = -2 + 5k, \quad , y = 1 - 2k.$$

□

2. Exercise 1.50 from the book (rephrased here for clarity): A farmer pays \$1770 for horses and oxen. Each horse costs \$31, and each ox costs \$21. What are the possible numbers of horses and oxen that the farmer bought? (Note that you can't buy a negative number of animals.)

Proof. Let x be the number of horses, and y the number of oxen. We are looking for non-negative solutions to the equation $31x + 21y = 1770$. Applying the Euclidean algorithm, we have

$$\begin{aligned} 31 &= 21(1) + 10 \\ 21 &= 10(2) + 1 \\ 10 &= 1(10) = 0 \end{aligned}$$

Thus

$$1 = 21 - 10(2) = 21 - (31 - 21(1))(2) = 31(-2) + 21(3),$$

and so

$$1770 = 31(-3540) + 21(5310),$$

and hence our initial solution is $x_0 = -3540$ and $y_0 = 5310$. By Theorem 1.53, all solutions are of the form

$$x = -3540 + 21k, \quad y = 5310 - 31k.$$

In order for x to be positive, we need $k \geq 169$; for y to be positive, we need $k \leq 171$. Thus the possible k values are 169, 170, and 171, so our possible solutions are:

- 9 horses and 71 oxen,
- 30 horses and 40 oxen, and
- 51 horses and 9 oxen.

□

3. Given any natural numbers a and b, let $\mathrm{lcm}(a, b)$ denote the **least common multiple** of a and b. Prove Theorem 1.57: For any natural numbers a and b,

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab.$$

(Hint: Theorem 1.55 may be helpful.)

Proof. By definition, $\mathrm{lcm}(a, b)$ is the minimal multiple of both a and b, so there exist positive integers k, l such that

$$\mathrm{lcm}(a, b) = ak = bl.$$

Then Theorem 1.55 implies that

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = \gcd(a \cdot \mathrm{lcm}(a, b), b \cdot \mathrm{lcm}(a, b)) = \gcd(abl, abk) = ab \cdot \gcd(l, k).$$

There exist integers k', l' so that $k = \gcd(l, k)k'$ and $l = \gcd(l, k)l'$. Thus $\mathrm{lcm}(a, b) = a \gcd(l, k) \cdot k' = b \gcd(l, k) \cdot l'$. If $\gcd(l, k) \neq 1$, then $a \gcd(l, k) = b \gcd(l, k)$ is a smaller common multiple of a, b then $\mathrm{lcm}(a, b)$, a contradiction. Hence $\gcd(l, k) = 1$, so

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab \cdot \gcd(l, k) = ab.$$

□

4. Prove Lemma 2.8: If the natural numbers p, q_1, $\ldots$, q_n are all prime, and if p divides the product $q_1 \cdots q_n$, then $p = q_i$ for some $1 \leq i \leq n$. (Hint: Use induction on n.)

   Proof. We go by induction on n. In the base case, for $n = 1$, we have $p|q_1$, and since q is prime, the only divisor of q_1 bigger than 1 is q_1 itself. Since $p > 1$, $p = q_1$.

   Suppose for induction that the result holds for all primes p and lists of n primes q_1, $\ldots$, q_n. Now, let p, q_1, $\ldots$, q_{n+1} be prime, and suppose $p|q_1 \cdots q_{n+1}$. We split into two cases. First, if $p = q_{n+1}$, then $p = q_i$ for $i = n+1$. Otherwise, by the base case, we have that $\gcd(p, q_{n+1}) = 1$. Thus, Theorem 1.41 implies that $p|q_1 \cdots q_n$, so by the induction hypothesis, $p = q_i$ for some $1 \leq i \leq n$. $\square$