Homework 3 Solutions

Tim Smits

1. Use the Euclidean Algorithm to find the greatset common divisors of the following pairs of integers:

(a) $(105, 56)$

(b) $(162, 47)$

(c) $(-2485, 1704)$

(d) $(924, 1960)$

(e) $(-8120, -14355)$

Solution: Run the Euclidean algorithm to compute the gcd. The details are omitted.

(a) $\gcd(105, 56) = 7$.

(b) $\gcd(162, 47) = 1$.

(c) $\gcd(-2485, 1704) = 71$.

(d) $\gcd(924, 1960) = 28$.

(e) $\gcd(-8120, -14355) = 145$.

2. Let $a, b \neq 0$ be integers, and set $g = \gcd(a, b)$. Show that any common divisor of a and b must divide g.

Solution: Let d be a common divisor of a and b, so that $d \mid a$ and $d \mid b$. By Bezout, there exist integers x and y such that $ax + by = g$. Since $d \mid a$ and $d \mid b$, there are integers a', b' such that $a = a'd$ and $b = b'd$. Then $g = d(a'x + b'y)$, so that $d \mid g$ as desired.

3. Set $a = a'g$ and $b = b'g$ for some integers a', b' with $g = \gcd(a, b)$. Show that $\gcd(a', b') = 1$.

Solution: Write $a = a'g$ and $b = b'g$ for some integers a', b'. By Bezout, there are integers x, y such that $ax + by = g$, so that $g(a'x + b'y) = g$. Dividing through by g says $a'x + b'y = 1$. Let $g' = \gcd(a', b')$. Since $g' \mid a'$ and $g' \mid b'$, we see $g' \mid a'x + b'y = 1$, so that $g' = 1$.

4. Use the extended Euclidean algorithm to find integers x, y such that $ax+by = g$ for $g = \gcd(a, b)$ for the following pairs of integers:

(a) $(509, 94)$

(b) $(-1260, 816)$

Solution: Run the Euclidean algorithm and use back substitution to write the greatest common divisor as a linear combination of a and b. The details are omitted.

(a) $(x, y) = (41, -222)$.

(b) $(x, y) = (11, 17)$.

5. Let $a, b \in \mathbb{Z}$ and Let $g = \gcd(a, b)$.

(a) Show that if $k \in \mathbb{Z}$, then $gk \in I(a, b)$.

(b) Show that if $n \in I(a, b)$ that $g \mid n$.

Solution:

(a) Let $k \in \mathbb{Z}$. By Bezout's lemma, we have $g \in I(a, b)$, so there are integers x, y such that $ax + by = g$. Then $gk = a(xk) + b(yk)$, so that $gk \in I(a, b)$.

(b) Suppose that $n \in I(a, b)$. Then there are integers x, y such that $n = ax + by$. Since $g \mid a$ and $g \mid b$, we may write $a = a'g$ and $b = b'g$ for some integers a', b'. Then $n = g(a'x + b'y)$, so that $g \mid n$.

6. Let a, b be relatively prime integers. Suppose we have an integer solution (x_0, y_0) to the equation $ax + by = 1$. For $k \in \mathbb{Z}$, define $x_k = x_0 + bk$ and $y_k = y_0 - ak$.

(a) Show that for all k, $ax_k + by_k = 1$.

(b) Let (x, y) be another solution to $ax + by = 1$. Show that $x = x_k$ and $y = y_k$ for some k.

Solution:

(a) We have $ax_k + by_k = a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 = 1$, since (x_0, y_0) is a solution to $ax + by = 1$ by assumption.

(b) Let (x, y) be an arbitrary solution to $ax + by = 1$. Since $ax_0 + by_0 = 1$, subtracting says $a(x - x_0) + b(y - y_0) = 0$, i.e. $a(x - x_0) = b(y_0 - y)$. Since a divides the left hand side, it also divides $b(y_0 - y)$, and since $\gcd(a, b) = 1$, the generalized version of Euclid's lemma says that $a \mid (y_0 - y)$. Similarly, we see $b \mid (x - x_0)$. Then $y_0 - y = as$ for some integer s, and $x - x_0 = at$ for some integer t, i.e. $y = y_0 - as$ and $x = x_0 + at$. Plugging into the equation $ax + by = 1$, we see that $ax_0 + abt + by_0 - abs = 1$, so that $abt - abs = 0$. This then implies that $s = t$, so setting these equal to a common parameter k shows that $x = x_k$ and $y = y_k$ for some k as desired.

7. Let $a, b \neq 0$ be integers with $g = \gcd(a, b)$. Suppose we have an integer solution (x_0, y_0) to $ax + by = g$. For $k \in \mathbb{Z}$, define $x_k = x_0 + b'k$ and $y_k = y_0 - a'k$ where $a = a'g$ and $b = b'g$ for some integers a', b'.

(a) For all $k \in \mathbb{Z}$, show that $ax_k + by_k = g$.

(b) Let (x, y) be another solution to $ax + by = 1$. Show that $x = x_k$ and $y = y_k$ for some k.

Solution:

(a) Write $a = a'g$ and $b = b'g$ for some integers a', b' with $g = \gcd(a, b)$. We have $ax_k + by_k = a(x_0 + b'k) + b(y_0 - a'k) = ax_0 + by_0 + ab'k - ab'k = 1 + ga'b'k - ga'b'k = 1$.

(b) Let (x, y) be an arbitrary solution to $ax + by = g$. Then write $a = a'g$ and $b = b'g$ for some integers a', b', so that $g(a'x + b'y) = g$. Dividing through by g says $a'x + b'y = 1$, so applying problem 8 says $x = x_0 + b'k$ and $y = y_0 - a'k$ for some k, i.e. $x = x_k$ and $y = y_k$.

8. Write the set of integer solution to the equation $509x + 94y = 1$ in set notation.

Solution: Use the fundamental solution $(x_0, y_0) = (41, -222)$ from 4a and problem 6 to conclude any solution (x, y) is of the form $x = 41 + 94k$ and $y = -222 - 509k$ for some k. Since each choice of k gives a solution, the solution set can be written as $S = \{(41 + 94k, -222 - 509k) : k \in \mathbb{Z}\}$.

9. Write the set of integer solutions to the equation $-1260x + 816y = 12$ in set notation.

Solution: Use the fundamental solution $(x_0, y_0) = (11, 17)$ from 4b and problem 7 to see every solution is of the form $x = 11 + 68k$ and $y = 17 + 105k$ for some integer k. Each choice of k gives a solution, so the solution set can be written as $S = \{(11 + 68k, 17 + 105k) : k \in \mathbb{Z}\}$.

10. Let $S \subset \mathbb{N}$ be a set with the property that S does not contain a least element. Use strong induction to show that S is empty. How does this prove the Well-Ordering Principle?

Solution: Note that $0 \notin S$ since 0 is the smallest natural number, so if it were in S then S would have a smallest element, and we said it doesn't. Now suppose for some k that $0, 1, \ldots, k \notin S$. Then $k + 1 \notin S$, because if it were, then it would be a least element of S, since all the naturals smaller than S are not contained in S, a contradiction to the assumption that S has no least element. Therefore by induction, this says $n \notin S$ for all $n \geq 0$, so that S is empty. We have shown that if $S \subset \mathbb{N}$ has no least element, that S must be empty, so taking the contrapositive says that if S is non-empty, that S has a least element, precisely the statement of the Well-Ordering Principle.