**Geoffrey Parker - grp352**
**HW 6: 1.38-1.40, 1.48, 1.50, 1.51, 1.53, 1.54**
**M328K**
**February 7th, 2012**

**1.38 Theorem.** *Let $a$ and $b$ be integers. If $(a, b) = 1$, then there exist integers $x$ and $y$ such that $ax + by = 1$.*

*Proof.* Let $a$ and $b$ be integers with $(a, b) = 1$. We will show that there exist integers $x$ and $y$ such that $ax + by = 1$. First, let $S$ be the set of natural numbers of the form $ax + by$ for any integers $x$ and $y$. Now we will show that $S$ is not empty. Because $(a, b) = 1$, $a$ and $b$ cannot both be 0, so assume that $|a| > 0$. If $a$ is positive, then $a1 + b0$ will be in $S$, and if $a$ is negative, then $a(-1) + b0$ will be an element of $S$.

Since $S$ is a non-empty subset of the natural numbers, then by the Well Ordering Axiom $S$ has a least element, which we will call $k$. Since $k$ is an element of $S$, it can be expressed as $k = ax_0 + bx_0$ for some integers $x_0$ and $y_0$. Then by the Division Algorithm there exist integers $q$ and $r$ such that $a = qk + r$ and $0 \leq r < k$. By substitution, this gives us $a = q(ax_0 + by_0) + r$, so $r = a - q(ax_0 + by_0) = a(1 - qx_0) + b(y_0)$. Now if we let $x_1 = 1 - qx_0$ and $y_1 = y_0$, then we see that $r = ax_1 + by_1$. Assume by way of contradiction that $r > 0$. In this case, $r$ is a natural number, and thus an element of the set $S$. However $r < k$, which is the least element of the set $S$, so we have a contradiction. Because $0 \leq r$ and not $r > 0$, $r$ must be 0. Therefore $a = qk$, and so $k \mid a$. By similar logic, we can also establish that $k \mid b$. Now we have that $k \mid a$ and $k \mid b$, so $k$ is a common divisor of $a$ and $b$. However, because $(a, b) = 1$, it must be that $k \leq 1$. And because $k$ is an element of $S$, which is a subset of the natural numbers, $k \geq 1$. Therefore $k = ax_0 + by_0 = 1$. □

**1.39 Theorem.** *Let $a$ and $b$ be integers. If there exist integers $x$ and $y$ with $ax+by = 1$, then $(a, b) = 1$.*

*Proof.* Let $a$, $b$, $x$, and $y$ with $ax + by = 1$. We will show that $(a, b) = 1$. First, let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, then by theorem 1.6 $d \mid ax$ and $d \mid ay$. So by theorem 1.1, $d \mid ax + by$, meaning $d \mid 1$. Because $d = (a, b)$, $d$ cannot be 0. Therefore $d = (a, b) = 1$. □

**1.40 Theorem.** *For any integers $a$ and $b$ not both 0, there are integers $x$ and $y$ such that*

$$ax + by = (a, b).$$

*Proof.* Let $a$ and $b$ be integers not both 0. First, we will redifine the Euclidean Algorithm as a collection of sequences, with a couple of extensions. Call it the Extended Euclidean Algorithm. Let $i$, $j$, $q$, $r$, $x$, and $y$ be sequences of integers, defined as follows: $i_k = j_{k-1}$, $j_k = r_{k-1}$, use the division algorithm to find $q_k$ and $r_k$ such that $i_k = j_k q_k + r_k$, $x_k = x_{k-2} - q_k x_{k-1}$, and $y_k = y_{k-2} - q_k y_{k-1}$. Now take these initial values: $i_2 = a$, $j_2 = b$, $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, and $y_1 = 1$. In effect, by filling out these sequences until you find a $k$ such that $r_k = 0$, you are performing the Euclidean Algorithm. In addition, we will use induction to prove that for any $k \geq 2$, $r_k = ax_k + by_k$.

As a base case, take $k = 2$ and $k = 3$. This gives us:

$$
\begin{aligned}
i_2 &= j_2 q_2 + r_2 \\
r_2 &= i_2 - q_2 j_2 \\
r_2 &= a - q_2 b \\
r_2 &= (ax_0 + by_0) - q_2(ax_1 + by_1) \\
r_2 &= a(x_0 - q_2 x_1) + b(y_0 + q_2 y_1) \\
r_2 &= ax_2 + by_2
\end{aligned}
$$

$$
\begin{aligned}
i_3 &= j_2 \\
j_3 &= r_2 \\
i_3 &= j_3 q_3 + r_3 \\
r_3 &= i_3 - q_3 j_3 \\
r_3 &= b - q_3 r_2 \\
r_3 &= (ax_1 + by_1) - q_3(ax_2 + by_2) \\
r_3 &= a(x_1 - q_3 x_2) + b(y_1 - q_3 y_2) \\
r_3 &= ax_3 + by_3
\end{aligned}
$$

Our induction hypothesis is that there exists some integer $N \geq 3$ such that $r_N = ax_N + by_N$. We must now show that $r_{N+1} = ax_{N+1} + by_{N+1}$.

$$
\begin{aligned}
r_N &= ax_N + by_N \\
i_{N+1} &= j_N \\
j_{N+1} &= r_N \\
i_{N+1} &= q_{N+1} j_{N+1} + r_{N+1} \\
r_{N+1} &= i_{N+1} - q_{N+1} j_{N+1} \\
r_{N+1} &= r_{N-1} - q_{N+1} r_N \\
r_{N+1} &= (ax_{N-1} + by_{N-1}) - q_{N+1}(ax_N + by_N) \\
r_{N+1} &= a(x_{N-1} - q_{N+1} x_N) + b(y_{N-1} - q_{N+1} y_N) \\
r_{N+1} &= ax_{N+1} + by_{N+1}
\end{aligned}
$$

Now suppose we let $M$ be an integer such that $r_M = 0$. Since this is the Euclidean Algorithm such an $M$ must exist, and this means that $(a, b) = j_M = r_{M-1} = ax_{M-1} + by_{M-1}$. □

**1.48 Theorem.** *Given integers $a$, $b$, and $c$ with $a$ and $b$ not both 0, there exist integers $x$ and $y$ that satisfy the equation $ax + by = c$ if and only if $(a, b)|c$.*

*Proof.* Let $a$, $b$, and $c$ be integers with $a$ and $b$ not both 0.

First assume $(a, b)|c$. Then, by theorem 1.40, there exist integers $x_0$ and $y_0$ that satisfy $ax_0 + by_0 = (a, b)$. And by the definition of divides, $c = (a, b)k$ for some integer $k$. So $c = k(ax_0 + by_0) = ax_0k + by_0k$. Let the integers $x$ and $y$ be $x_0k$ and $y_0k$. Therefore $ax + by = c$.

Now assume by way of contradiction that $ax + by = c$ and $(a, b) \nmid c$. Let $d = (a, b)$. Then by the definition of divides, there exist integers $j$ and $k$ such that $c = jdx + kdy = d(jx + ky)$. Since $(jx + ky)$ is an integer, $d \mid c$, which contradicts our assumption. Therefore if $ax + by = c$, then $(a, b) \mid c$. □

**1.50 Exercise** (Euler)**.** *A farmer lays out the sum of* $1,770$ *crowns in purchasing horses and oxen. He pays* $31$ *crowns for each horse and* $21$ *crowns for each ox. What are the possible numbers of horses and oxen that the farmer bought?*

*Solution.* Let $x$ be the number of horses and $y$ be the number of oxen. So $1770 = 31x + 21y$.
$x = 9$, $y = 71$
$x = 30$, $y = 40$
$x = 51$, $y = 9$ □

**1.51 Theorem.** *Let $a$, $b$, $c$, $x_0$, and $y_0$ be integers with $a$ and $b$ not both 0 such that $ax_0 + by_0 = c$. Then the integers*

$$x = x_0 + \frac{b}{(a,b)} \text{ and } y = y_0 - \frac{a}{(a,b)}$$

*also satisfy the linear Diophantine equation $ax + by = c$.*

*Proof.* Let $a$, $b$, $c$, $x_0$, and $y_0$ be integers with $a$ and $b$ not both 0 such that $ax_0+by_0 = c$. Also let $x = x_0+\frac{b}{(a,b)}$ and $y = y_0-\frac{a}{(a,b)}$. So all the following equations are equivalent:

$$\begin{gathered} ax_0 + by_0 \\ ax_0 + by_0 + \frac{ab}{(a,b)} - \frac{ab}{(a,b)} \\ ax_0 + \frac{ab}{(a,b)} + by_0 - \frac{ab}{(a,b)} \\ a(x_0 + \frac{b}{(a,b)}) + b(y_0 - \frac{a}{(a,b)}) \\ ax + by \end{gathered}$$

Therefore $ax + by = c$.

□

**1.53 Theorem.** *Let $a$, $b$, and $c$ be integers with $a$ and $b$ not both 0. If $x = x_0$, $y = y_0$ is an integer solution to the equation $ax + by = c$ (that is, $ax_0 + by_0 = c$) then for every integer $k$, the numbers*

$$x = x_0 + \frac{kb}{(a,b)} \text{ and } y = y_0 - \frac{ka}{(a,b)}$$

*are integers that also satisfy the linear Diophantine equation $ax + by = c$. Moreover, every solution to the linear Diophantine equation $ax + by = c$ is of this form.*

*Proof.* Let $a$, $b$, and $c$ be integers with $a$ and $b$ not both 0. Let $S$ be the set of all pairs of integers $\langle x, y\rangle$ such that $x$ and $y$ satisfy the equation $ax+by = c$. Let $\langle x_0, y_0\rangle$ be an element of $S$. Let $x_k = x_0 + \frac{kb}{(a,b)}$ and $y_k = y_0 - \frac{ka}{(a,b)}$. We will show both that for all $k$, $\langle x_k, y_k\rangle$ is an element of $S$ and that all elements of $S$ may be expressed in the form $\langle x_k, y_k\rangle$.

First, for any $\langle x_k, y_k \rangle$, the following equations are equivilant.

$$\begin{aligned} & ax_k + by_k \\ & a(x_0 + \frac{kb}{(a,b)}) + b(y_0 - \frac{ka}{(a,b)}) \\ & ax_0 + \frac{akb}{(a,b)} + by_0 - \frac{bka}{(a,b)} \\ & ax_0 + by_0 + \frac{abk}{(a,b)} - \frac{abk}{(a,b)} \\ & ax_0 + by_0 \end{aligned}$$

Since $ax_0 + by_0 = c$, $ax_k + by_k = c$, so $\langle x_k, y_k \rangle$ is an element of S.

Now consider any pair of integers $\langle x', y' \rangle$ which is an element of $S$. Once again, the following equations are all equivalent.

$$\begin{aligned} & ax' + by' \\ & ax' + by' + \frac{abk}{(a,b)} - \frac{abk}{(a,b)} && \textit{for some integer } k \\ & ax' + \frac{akb}{(a,b)} + by' - \frac{bka}{(a,b)} \\ & a(x' + \frac{kb}{(a,b)}) + b(y' - \frac{ka}{(a,b)}) \\ & ax_k + by_k \end{aligned}$$

Therefore any pair of integers $\langle x', y' \rangle$ in $S$ can be expressed as $\langle x_k, y_k \rangle$. □

**1.54 Exercise.** *Find all integer solutions to the equation* $24x + 9y = 33$.

*Proof.* Using the Extended Euclidean Algorithm from theorem 1.40, we find that $3 = 24(-1) + 9(3)$, where $(24, 9) = 3$. From here we see that $33 = (3)11 = 3(24(-1) + 9(3)) = 24(-3) + 9(9)$. Therefore by theorem 1.53, we see that all integer solutions to the equation $24x + 9y = 33$ will be of the form $x_k = -3 + \frac{k9}{3} = -3 + 3k$ and $y_k = 9 - \frac{k24}{3} = 9 - 8k$. □