Geoffrey Parker - grp352
HW 5: 1.38-1.43, 1.45
M328K
February 2nd, 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 $(a, b) = 1$. Since $(a, b) = 1$, it must be the case that a and b are not both 0. Therefore by theorem 1.40, there exist integers x and y such that $1 = (a, b) = ax + by$. $\square$

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 be integers with $ax + by = 1$. We will show that $(a, b) = 1$. This is true by theorem 1.40. $\square$

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 $i_k = j_k q_k + r_k$, $x_k = x_{k-2} - x_{k-1}$, and $y_k = y_{k-2} - y_{k-1}$. Now take these initial values: $i_2 = a$, $j_2 = b$, $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, and $y_1 = 1$. Also let $r_1 = j_2$. 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 $k = 2$. This gives us:

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

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, this means that $(a, b) = j_M = r_{M-1} = ax_{M-1} + by_{M-1}$. $\square$

1.41 Theorem. *Let a, b, and c be integers. If $a|bc$ and $(a, b) = 1$, then $a|c$.*

Proof. Let a, b, and c be integers with $a \mid bc$ and $(a, b) = 1$. We will show $a \mid c$. First, if $a = 1$, then $a \mid c$ because 1 divides all integers. And a can not be 0 because then (a, b) would be 0. Now consider the case of $|a| > 1$. Suppose by way of contradiction that $a \mid b$. Then $|a| \mid a$ and $|a| \mid b$, and because $|a| > 1$, $|a| > (a, b)$, which is a contradiction. So $a \nmid b$. Therefore $a \mid c$ $\square$

1.42 Theorem. *Let a, b, and n be integers. If $a|n$, $b|n$ and $(a,b)=1$, then $ab|n$.*

Proof. Let a, b, and n be integers with $a \mid n$, $b \mid n$ and $(a,b)=1$. We will show that $ab \mid n$. Consider the sets A of integers that a divides and B the integers that b divides. Let $S = A \cap B$. S is the set of all integers of the form abk. Since n is an element of S, $ab \mid n$. □

1.43 Theorem. *Let a, b, and n be integers. If $(a,n)=1$ and $(b,n)=1$, then $(ab,n)=1$.*

Proof. Let a, b, and n be integers with $(a,n)=1$ and $(b,n)=1$. We will show that $(ab,n)=1$. Let $d=(ab,n)$. Assume by way of contradiction that $d>1$. However, since $(a,n)=1$ and $(b,n)=1$, it must be the case that $d \nmid a$ and $d \nmid b$. □

1.45 Theorem. *Let a, b, c and n be integers with $n>0$. If $ac \equiv bc \pmod{n}$ and $(c,n)=1$, then $a \equiv b \pmod{n}$.*

Proof. Let a, b, c and n be integers with $n>0$, $ac \equiv bc \pmod{n}$, and $(c,n)=1$. We will show that $a \equiv b \pmod{n}$. First, by definition of congruence mod n, $n \mid (ac-bc)$, so $n \mid c(a-b)$. Since $(n,c)=1$, then by theorem 1.41 $n \mid (a-b)$. Therefore by definition of conguence mod n, $a \equiv b \pmod{n}$. □