Geoffrey Parker - grp352
HW 4: 1.29-1.37
M328K
January 31st, 2012

1.26 Theorem. *Prove the existence part of the Division Algorithm. (Hint: Given n and m, how will you define q? Once you choose this q, then how is r chosen? Then show that $0 \leq r \leq n-1$.)*

Proof. Let n and m be natural numbers. Let S be the set of natural numbers of the form $m - nk + 1$ for some integer k. Since m is a natural number, S always has at least one member, $m - n0 + 1$. Therefore by the Well-Ordering Axiom for the natural numbers, there exists a smallest element of the set S. Let q be an integer such that $m - nq + 1$ is this smallest element. Let $r = m - nq$. So $m = nq + r$. Now we will show that $0 \leq r \leq n-1$. Since r is defined to be drawn from a subset of the natural numbers, $r \geq 0$. Assume by way of contradiction that $r \geq n$. This would mean that $m - nq \geq n$, or $m - nq - n \geq 0$. So $m - n(q+1) \geq 0$, which makes $m - n(q+1) + 1$ an element of S. But $m - n(q+1) + 1 < m - nq + 1$, which is a contradiction, since $m - nq + 1$ is the smallest element of S. Therefore $r < n$, or, since r and n are integers, $r \leq n-1$. So we have proved that $0 \leq r \leq n-1$. □

NOTE TO READER: The well ordering axiom we have is only defined on the natural numbers, which is why there are +1's every time S is mentioned.

1.27 Theorem. *Prove the uniqueness part of the Division Algorithm.*

(Hint: If $nq + r = nq' + r'$, then $nq - nq' = r' - r$. Use what you know about r and r' as part of your argument that $q = q'$.)

Proof. Let there be integers $m,\ n,\ q,\ r,\ q',\ r'$ such that $m = nq + r$, $m = nq' + r'$, $0 \leq r \leq n$, and $0 \leq r' \leq n$. Given this, $nq + r = nq' + r'$, or $r - r' = nq' - nq = n(q' - q')$, which means that $n \mid (r - r')$. So by the definition of divides, there exists some integer k such that $nk = r - r'$. However, $\leq r \leq n$ and $0 \leq r' \leq n$, so $-n < r - r' < n$, which means that k must be 0 and $r - r'$ must be 0. Therefore $r = r'$. Going back to $r - r' = n(q' - q')$, we can say that $n(q' - q') = 0$. Since n is a natural number, and thus not 0, $q' - q$ must be 0. Therefore $q = q'$. □

1.29 Question. *Do every two integers have at least one common divisor?*

Solution. Yes. One divides every integer, so for any two integers a and b, $1 \mid a$ and $1 \mid b$. $\square$

1.30 Question. *Can two integers have infinitely many common divisors?*

Solution. No. For any two integers a and b, any common divisor of a and b must divide a. And all of a's divisors must be between $-a$ and a, which is a finite range. So it is impossible for two integers to have infinitely many common divisors. $\square$

1.31 Exercise. *Find the following greatest common divisors. Which pairs are relatively prime?*

(1) $(36, 22) = 2$

(2) $(45, -15) = 15$

(3) $(-296, -88) = 8$

(4) $(0, 256) = 256$

(5) $(15, 28) = 1$. 15 *and* 28 *are relatively prime.*

(6) $(1, -2436) = 1$. 1 *and* -2436 *are relatively prime.*

1.32 Theorem. *Let a, n, b, r, and k be integers. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.*

Proof. Let a, n, b, r, and k be integers with $a = nb + r$ and $k|a$ and $k|b$. We will show that $k|r$. First, because $k|a$ and $k|b$, then by the definition of divides $a = kj$ and $b = km$ for some integers k and m. So $kj = nkm + r$ and $kj - nkm = r$, which means that $r = k(j - nm)$. Since j, n, and m are integers, $j - nm$ is an integer. Therefore, by the definition of divides, $k \mid r$. $\square$

1.33 Theorem. *Let a, b, n_1, and r_1 be integers with a and b not both 0. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.*

Proof. Let a, b, n_1, and r_1 be integers with a and b not both 0 and $a = n_1 b + r_1$. We will show that $(a, b) = (b, r_1)$. Let $d = (a, b)$. By definition of greatest common divisor, d is the largest integer such that $d \mid a$ and $d \mid b$. By theorem 1.32, this means that $d \mid r_1$, so d is a common divisor of b and r_1. Suppose there were some other common divisor of b and r_1 x, such that $x > d$. This would mean $x \mid b$ and $x \mid r_1$, so by definition of divides, there exist integers j and k such that $b = xj$ and $r_1 = xk$. This gives us $a = n_1 xj + xk = x(n_1 j + k)$. Since $n_1 j + k$ is an integer, $x \mid a$. So x is a common divisor of both a and b. However, we have already established that d is the greatest common divisor of a and b, and $x > d$. We have a contradiction. Therefore, d is the greatest common divisor of b and r_1, and so $(a, b) = (b, r_1)$. □

1.34 Exercise. *As an illustration of the above theorem, note that*

$$\begin{aligned} 51 &= 3 \cdot 15 + 6, \\ 15 &= 2 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Use the preceding theorem to show that if $a = 51$ and $b = 15$, then $(51, 15) = (6, 3) = 3$.

Solution. Since $51 = 3 \cdot 15 + 6$, then by theorem 1.33 $(51, 15) = (15, 6)$. And because $15 = 2 \cdot 6 + 3$, then by theorem 1.33 $(15, 6) = (6, 3)$. Once again by theorem 1.33, because $6 = 2 \cdot 3 + 0$, $(6, 3) = (3, 0)$, which equals 3. So $(51, 15) = (6, 3) = 3$. □

1.35 Exercise (Euclidean Algorithm)**.** *Using the previous theorem and the Division Algorithm successively, devise a procedure for finding the greatest common divisor of two integers.*

Solution. Given two integers a and b find (a, b).

1. Let i and j be integers. If $|a| \geq |b|$, let $i = a$ and $j = b$, otherwise let $i = b$ and $j = a$.
2. If $j = 0$, then $(a, b) = i$. Stop the procedure, you are finished.
3. By the division algorithm, there exist integers q and r such that $i = jq + r$ where $0 \leq r \leq j - 1$. Find q and r.
4. By theorem 1.33, $(i, j) = (j, r)$. If $r = 0$, then $(a, b) = |j|$. Stop the procedure, you are finished. Otherwise, let $i = j$ and $j = r$ and goto step 3.

$\square$

1.36 Exercise. *Use the Euclidean Algorithm to find*

(1) $(96, 112)$

Solution.

1. Let $i = 112$, $j = 96$.
2. $j \neq 0$.
3. $q = 0$, $r = 16$.
4. $r \neq 0$ so $i = 96$ and $j = 16$.
5. $q = 6$ and $r = 0$.
6. $r = 0$ so $(96, 112) = 16$.

$\square$

(2) $(162, 31)$

Solution.

1. Let $i = 162$, $j = 31$.
2. $j \neq 0$.
3. $q = 5$, $r = 7$.
4. $r \neq 0$ so $i = 31$ and $j = 7$.
5. $q = 4$ and $r = 3$.
6. $r \neq 0$ so $i = 7$ and $j = 3$.
7. $q = 2$ and $r = 1$.
8. $r \neq 0$ so $i = 3$ and $j = 1$.
9. $q = 3$ and $r = 0$.
10. $r = 0$ so $(162, 31) = 1$.

$\square$

(3) $(0, 256)$

Solution.

1. Let $i = 256$ and $j = 0$
2. $j = 0$. $(0, 256) = 256$

$\square$

(4) $(-288, -166)$

Solution.

1. Let $i = -288$, $j = -166$.
2. $j \neq 0$
3. $q = 1$, $r = -122$.
4. $r \neq 0$ so $i = -166$ and $j = -122$.
5. $q = 1$ and $r = -44$.
6. $r \neq 0$ so $i = -122$ and $j = -44$.
7. $q = 2$ and $r = -34$.
8. $r \neq 0$ so $i = -44$ and $j = -34$.
9. $q = 1$ and $r = -10$.
10. $r \neq 0$ so $i = -34$ and $j = -10$.
11. $q = 3$ and $r = -4$.
12. $r \neq 0$ so $i = -10$ and $j = -4$.
13. $q = 2$ and $r = -2$.
14. $r \neq 0$ so $i = -4$ and $j = -2$.
15. $q =$ and $r = 0$.
16. $r = 0$ so $(-288, -166) = 2$.

$\square$

(5) $(1, -2436)$

Solution.

1. Let $i = -2436$ and $j = 1$
2. $j \neq 0$
3. $q = -2436$ and $r = 0$
4. $r = 0$ so $(1, -2436) = 1$.

$\square$

1.37 Exercise. *Find integers x and y such that $162x + 31y = 1$.*

Solution. $162 \cdot 9 + 31 \cdot -47 = 1$. $\square$