Section 4.2: The Division Algorithm and Greatest Common Divisors

The Division Algorithm

The Division Algorithm is merely long division restated as an equation. For example, the division

\[
\begin{array}{c|c}
32 & r, 20 \\
\hline
32 & 948 \\
\end{array}
\]

can be rewritten in equation form as \( 948 = 32(29) + 20 \).

More generally, if \( m \) (the dividend) and \( d \) (the divisor) are positive integers then division of \( m \) by \( d \) yields quotient \( q \) and remainder \( r \) as follows:

\[
\begin{array}{c|c}
q & \text{rem} r \\
\hline
\text{d} & m \\
\end{array}
\]

Furthermore, we know that \( 0 \leq r < d \).

We can express (**) in equation form as:

\[
m = dq + r \quad \text{where} \quad 0 \leq r < d.
\]

Theorem 1 (The Division Algorithm for Integers): Let \( m \) be any integer and let \( d \) be a positive integer. Then there exist unique integers \( q \) and \( r \) such that \( 0 \leq r < d \) and \( m = dq + r \).

Comment: Note that in the Division Algorithm, \( m \), the dividend, is an arbitrary integer. From long division, we are familiar only with the case where \( m \geq d \). The other cases are easily handled as follows.

Case 1: Assume \( 0 \leq m < d \). Then set \( q = 0 \) and \( r = m \); that is, \( m = d(0) + m \).

Case 2: Assume the dividend is \( -m \), where \( m \) is positive. Since \( m \) is positive, we can use long division to find integers \( q \) and \( r \) such that \( m = dq + r \). Then \( -m = d(-q) - r = d(-q - 1) + (d - r) \). Since \( 0 \leq r < d \), it follows that \( 0 \leq d - r < d \).

Exercise 1: In each of (a) – (d) you are given values for \( m \) and \( d \). In each case find (using the notation of the Division Algorithm) the quotient \( q \) and the remainder \( r \).

(a) \( m = 6, d = 10 \) \quad (b) \( m = -6, d = 10 \)

(c) \( m = 15153, d = 83 \) \quad (d) \( m = -15153, d = 83 \)
Greatest Common Divisors

**Definition 1:** Let $a$ and $b$ be integers. A positive integer $d$ is called the greatest common divisor of $a$ and $b$, written $d = \gcd(a, b)$, provided:

(a) $d$ divides $a$ and $d$ divides $b$; and

(b) if $c$ is an integer such that $c$ divides $a$ and $c$ divides $b$, then $c$ divides $d$.

**Comment:** In words, the definition states that $d = \gcd(a, b)$ provided $d$ is a common divisor of $a$ and $b$ and $d$ is divisible by all other common divisors of $a$ and $b$.

**Example 1:** The common divisors of 18 and 30 are $\pm 1$, $\pm 2$, $\pm 3$, and $\pm 6$. Clearly, $6 = \gcd(18, 30)$ and note that all other common divisors of 18 and 30 divide 6.

**Uniqueness of the GCD**

**Lemma 1:** Let $d_1$ and $d_2$ be positive integers such that $d_1$ divides $d_2$ and $d_2$ divides $d_1$. Then $d_1 = d_2$.

**Proof:** Let $d_1$ and $d_2$ be positive integers such that $d_1$ divides $d_2$ and $d_2$ divides $d_1$. Then there exist positive integers $q_1$ and $q_2$ such that $d_1 = q_1d_2$ and $d_2 = q_2d_1$. Thus,

$$d_1 = q_1d_2 = q_1(q_2d_1) = (q_1q_2)d_1.$$ 

Since $d_1 = (q_1q_2)d_1$, it follows that $1 = q_1q_2$. Recall that $q_1$ and $q_2$ are both positive, so it follows that $q_1 = q_2 = 1$. (The only other possibility, $q_1 = q_2 = -1$, is eliminated.) Thus, $d_1 = q_1d_2 = d_2$.

**Theorem 2:** Let $a$ and $b$ be integers. If $\gcd(a, b)$ exists, it is unique.

**Proof:** Let $a$ and $b$ be integers and assume that $\gcd(a, b)$ exists. Suppose that $d_1 = \gcd(a, b)$ and suppose also that $d_2 = \gcd(a, b)$. Let’s first view $d_1$ as $\gcd(a, b)$. Since $d_2$ is, by (a) of Definition 1, a common divisor of $a$ and $b$, it follows from (b) of Definition 1 that $d_2$ divides $d_1$. Similarly, viewing $d_2$ as $\gcd(a, b)$, we see that $d_1$ divides $d_2$. It now follows from Lemma 1 that $d_1 = d_2$, so $\gcd(a, b)$ is unique when it exists.
Existence of the GCD

Special Cases: Let $a$ and $b$ be integers.

- $\gcd(0, 0)$ does not exist.
- If $a \neq 0$ then $\gcd(a, 0) = |a|$.
- If $a$ divides $b$ then $\gcd(a, b) = |a|$.
- If $a \neq 0$ and $b \neq 0$ then $\gcd(a, b) = \gcd(|a|, |b|)$.

Thus, in the algorithm given as the proof of Theorem 3 below, we may always assume that $a$ and $b$ are positive integers.

The next Lemma gives an essential “reduction step” for calculating $\gcd(a, b)$.

**Lemma 2:** Let $a, b, q,$ and $r$ be integers such that $a = qb + r$. (cf. The Division Algorithm) Then $\gcd(a, b) = \gcd(b, r)$.

**Proof:** The proof of Lemma 2 is Exercise 4.2.3.

**Theorem 3:** If $a$ and $b$ are integers, not both zero, then $\gcd(a, b)$ exists.

**Proof:** The special cases were considered above. We give here an algorithm for finding $\gcd(a, b)$ when $a \geq b > 0$.

Apply the Division Algorithm, with $b$ as the divisor, to obtain

$$a = q_1 b + r_1 \text{ where } 0 \leq r_1 < b.$$  

If $r_1 \neq 0$, apply the Division Algorithm to $b$ and $r_1$, with $r_1$ as the divisor, to obtain

$$b = q_2 r_1 + r_2 \text{ where } 0 \leq r_2 < r_1.$$  

If $r_2 \neq 0$, apply the Division Algorithm to $r_1$ and $r_2$, with $r_2$ as the divisor, to obtain

$$r_1 = q_3 r_2 + r_3 \text{ where } 0 \leq r_2 < r_1.$$  

Since the remainders $r_1, r_2, r_3$, etc. form a sequence of positive integers with $r_1 > r_2 > r_3 \cdots \geq 0$. It follows that there is an integer $k$ such that $r_k \neq 0$ but $r_{k+1} = 0$.

Following is the algorithm for calculating $\gcd(a, b)$:
Algorithm 1: Finding the GCD:

\[ a = q_1 b + r_1 \text{ where } 0 \leq r_1 < b \]
\[ b = q_2 r_1 + r_2 \text{ where } 0 \leq r_2 < r_1 \]
\[ r_1 = q_3 r_2 + r_3 \text{ where } 0 \leq r_3 < r_1 \]
\[ \vdots \]
\[ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \text{ where } 0 \leq r_{k-1} < r_{k-2} \]
\[ r_{k-2} = q_k r_{k-1} + r_k \text{ where } 0 \leq r_k < r_{k-1} \]
\[ r_{k-1} = q_{k+1} r_k \]

Then \( r_k = \gcd(a, b) \).

To see that \( r_k = \gcd(a, b) \), repeatedly apply Lemma 2 to get
\[ \gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k). \]
But, by the last equation in Algorithm 1, \( r_k \) divides \( r_{k-1} \). Thus, \( r_k = \gcd(r_{k-1}, r_k) = \gcd(a, b) \).

Example 2: Find \( \gcd(216, 80) \).

Solution: Repeated use of long division gives:

\[
\begin{array}{cccccc}
2 & r & 56 & 1 & r & 24 \\
80 | 216 & 56 | 80 & 24 | 56 & 8 | 24 \\
56 & 80 & 24 & 56 & 8 & 24
\end{array}
\]

or, in equation form:

\[
216 = (2)80 + 56 \quad 80 = (1)56 + 24 \quad 56 = (2)24 + 8 \quad 24 = (3)8.
\]

Therefore, \( 8 = \gcd(216, 80) \).

Exercise 2: In each of (a) – (d), find \( \gcd(a, b) \).

(a) \( a = -44, b = 0 \) \quad (b) \( a = -22, b = 660 \)
(c) \( a = 715, b = 208 \) \quad (d) \( a = 715, b = -208 \)

Further Theorems

Theorem 4: Let \( a \) and \( b \) be integers and suppose \( d = \gcd(a, b) \). Then there exist integers \( m \) and \( n \) such that \( d = ma + nb \).

Comment: Note that \( 6 = \gcd(18, 30) \) and we may write
\[
6 = (2)18 + (-1)30 = (-3)18 + (2)30 = (7)18 + (-4)30,
\]
so, in the notation of Theorem 4, \( m \) and \( n \) are not unique.
The following algorithm for finding one choice for \( m \) and \( n \) is a continuation of Algorithm 1 for find \( \gcd(a, b) \).

**Algorithm 2: Writing \( \gcd(a, b) = ma + nb \)**

Beginning with the second to last equation of Algorithm 1 and working up, we solve each equation for the remainder. This gives:

\[
\begin{align*}
  r_k &= r_{k-2} - q_k r_{k-1} \\
  r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\
  & \vdots \\
  r_3 &= r_1 - q_3 r_2 \\
  r_2 &= b - q_2 r_1 \\
  r_1 &= a - q_1 b
\end{align*}
\]

Recall that \( r_k = \gcd(a, b) \).

In the equation for \( r_k \), substitute for \( r_{k-1} \), using the second equation. This gives

\[
\begin{align*}
  r_k &= r_{k-2} - q_k r_{k-1} \\
  &= r_{k-2} - q_k (r_{k-3} - q_{k-1} r_{k-2}) \\
  &= (1 + q_{k-1}) r_{k-2} + (-q_k) r_{k-3}.
\end{align*}
\]

In the resulting equation, we next substitute for \( r_{k-2} \) and simplify. Then substitute for \( r_{k-3} \) and simplify. Continuing, we eventually substitute for \( r_1 \) and simplify. This will yield \( r_k = ma + nb \).

**Example 3:** We have seen in Example 2 that \( 8 = \gcd(216, 80) \). Find integers \( m \) and \( n \) such that \( 8 = 216m + 80n \).

**Solution:** In the solution to Example 3 we obtained several equations representing the repeated applications of the Division Algorithm. In reverse order, we solve each those equations for the remainder. This gives:

\[
8 = 56 - (2)24 \quad 24 = 80 - (1)56 \quad 56 = 216 - (2)80.
\]

Now in \( 8 = 56 - (2)24 \) substitute \( 24 = 80 - (1)56 \) to obtain

\[
8 = 56 - 2(80 - (1)56) = (-2)80 + (3)56.
\]

Next, substitute \( 56 = 216 - (2)80 \) to obtain:

\[
8 = (-2)80 + (3)56 = (-2)80 + 3(216 - (2)80) = (3)216 - (8)80.
\]

Thus, \( 8 = (3)216 - (8)80 \).
**Exercise 3:** Find $d = \gcd(4977, 405)$ and find integers $m$ and $n$ such that $d = 4977m + 405n$.

**Theorem 5:** Let $a$, and $b$ be integers, where $a$ and $b$ are not both zero. Then $\gcd(a, b)$ exists so let $d = \gcd(a, b)$. For an integer $c$ there exist integers $m$ and $n$ such that $c = ma + nb$ if and only if $c$ is a multiple of $d$.

**Proof:** Note that this is an equivalence, so two proofs are required.

First, let $c$ be an integer and assume that there exist integers $m$ and $n$ such that $c = ma + nb$. Let $d = \gcd(a, b)$. Then $d$ divides both $a$ and $b$, so there exist integers $a_1$ and $b_1$ such that $a = a_1d$ and $b = b_1d$. Thus, $c = ma + nb = ma_1d + nb_1d = (ma_1 + nb_1)d$. Consequently, $c = qd$, where $q = ma_1 + nb_1$, and so $d$ divides $c$.

In the opposite direction, set $d = \gcd(a, b)$, let $c$ be an integer, and assume that $d$ divides $c$. Then there exists an integer $k$ such that $c = kd$. By Theorem 4, there exist integers $m_1$ and $n_1$ such that $d = m_1a + n_1b$. Therefore, $c = kd = k(m_1a + n_1b) = km_1a + kn_1b$. Thus, $c = ma + nb$, where $m = km_1$ and $n = kn_1$.

**Exercise 4:** Suppose $11 = ma + nb$, where $a$, $b$, $m$, and $n$ are integers. List all possible choices for $d = \gcd(a, b)$.
Section 4.2. EXERCISES

4.2.1. In each of (a) – (e) you are given integers \( m \) and \( n \), where \( n \) is positive. In each case, find integers \( q \) and \( r \) such that \( m = qn + r \) and \( 0 \leq r < n \).

(a) \( m = 2, n = 5 \)  
(b) \( m = -2, n = 5 \)  
(c) \( m = 30, n = 6 \)  
(d) \( m = 4129, n = 232 \)  
(e) \( m = -4129, n = 232 \).

4.2.2. In each of (a) – (c) below you are given integers \( a \) and \( b \). In each case use the Division Algorithm to find \( \text{gcd}(a, b) \) and to find integers \( m \) and \( n \) such that \( \text{gcd}(a, b) = ma + nb \)

(a) \( a = 899, b = 29 \)  
(b) \( a = 224, b = 98 \)  
(c) \( a = 963, b = 177 \)

4.2.3. Let \( a, b, q, \) and \( r \) be integers such that \( a = bq + r \). Prove that \( \text{gcd}(a, b) = \text{gcd}(b, r) \).

4.2.4. Let \( a, b, c, \) and \( d \) be integers such that \( a \) divides \( bc \) and \( d = \text{gcd}(a, b) \). Prove that \( a \) divides \( cd \).

4.2.5. Let \( a \) and \( b \) be integers and let \( d = \text{gcd}(a, b) \). If \( k \) is a positive integer, prove that \( kd = \text{gcd}(ka, kb) \).