1 Greatest Common Divisors and the Euclidean Algorithm

Definition 1 Suppose that \( a \) and \( b \) are integers, not both zero. The greatest common divisor of \( a \) and \( b \), denoted by gcd \((a,b)\), is defined to be the largest integer that divides both \( a \) and \( b \).

Example 2 Find the greatest common divisor of 48 and 60.

Solution 3 The factorization of 48 into prime factors is \( 48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \) and the factorization of 60 into prime factors is \( 60 = 2 \cdot 2 \cdot 3 \cdot 5 \). Thus the set of positive divisors of 48 is

\[
D(48) = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}
\]

and the set of positive divisors of 60 is

\[
D(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}.
\]

Since

\[
D(48) \cap D(60) = \{1, 2, 3, 4, 6, 12\},
\]

we see that \( \text{gcd}(48, 60) = 12 \).

Remark 4 Note that in finding \( \text{gcd}(a,b) \) we only need to consider the positive divisors of \( a \) and \( b \). This is because the greatest common divisor can’t be negative.
Example 5  Find the greatest common divisor of 68 and 114.

Solution 6  The factorization of 68 into prime factors is $68 = 2 \cdot 2 \cdot 17$ and the factorization of 114 into prime factors is $114 = 2 \cdot 3 \cdot 19$. Thus the set of positive divisors of 68 is

$$D(68) = \{1, 2, 4, 17, 34, 68\}$$

and the set of positive divisors of 114 is

$$D(114) = \{1, 2, 3, 6, 19, 38, 57, 114\}.$$  

Since

$$D(68) \cap D(114) = \{1, 2\},$$

we see that $\text{gcd}(68, 114) = 2$.

The method by which we found $\text{gcd}(48, 60)$ and $\text{gcd}(68, 114)$ in the previous two examples is rather tedious since it required us to find all of the positive common divisors of the two numbers in question. If the numbers $a$ and $b$ are very large, then this method of finding $\text{gcd}(a, b)$ is impractical. We are going to discover a better method, which is called the Euclidean Algorithm. It will be seen that the Euclidean Algorithm works because of the fact (which is not obvious) that $\text{gcd}(a, b)$ can always be written in the form $\text{gcd}(a, b) = ma + nb$ where $m$ and $n$ are integers. In other words, given any two positive integers $a$ and $b$, there will always exist two integers $m$ and $n$ such that $\text{gcd}(a, b) = ma + nb$. For example, we found that $\text{gcd}(48, 60) = 12$ and it is easily seen that

$$12 = (-1)(48) + (1)(60).$$

We also found that $\text{gcd}(68, 114) = 2$ and it is easily checked that

$$2 = (-5)(68) + (3)(114).$$

Of course, it is not obvious at this point how one comes up with the correct integers $m = -5$ and $n = 3$, but we will also address this question.

To begin our investigation of this topic, for two given integers $a$ and $b$, let the set $S$ be defined by

$$S = \{sa + tb \mid s \in \mathbb{Z}, t \in \mathbb{Z}, sa + tb > 0\}.$$
It is clear that $S \subseteq \mathbb{N}$ (since every member of $S$ is a positive integer) and it is also clear that $S \neq \emptyset$ because $a = (1) a + (0) b$, $-a = (-1) a + (0) b$, $b = (0) a + (1) b$, and $-b = (0) a + (-1) b$ and, since at least one of $a$ and $b$ is not zero, at least one of the numbers $a$, $-a$, $b$, $-b$ is a positive integer, so at least one of these numbers must be in $S$. By the Well–Ordering Principle, $S$ must have a smallest member, which we will call $d$. Since $d \in S$, we know that $d$ is a positive integer and that there exist integers $m$ and $n$ such that $d = ma + nb$. We are going to prove that, in fact, $d = \gcd (a, b)$.

**Theorem 7** Let the number $d$ be as defined in the preceding paragraph. Then $d = \gcd (a, b)$.

**Proof.** First we will prove that $d$ is a divisor of both $a$ and $b$. (We will actually just prove that $d$ is a divisor of $a$, since the proof that $d$ is a divisor of $b$ is similar.) Our proof that $d$ is a divisor of $a$ will be a proof by contradiction. (That is, we will assume that $d$ is not a divisor of $a$ and then arrive at a contradiction.)

Suppose that $d$ is not a divisor of $a$. Then, by the Division Algorithm, there exist integers $q$ and $r$ such that $a = qd + r$ and $0 < r < d$. (Note, it must be that $0 < r$ rather than $0 \leq r$ because we are assuming that $d$ is not a divisor of $a$.) Now, since $d = ma + nb$, we have

$$a = q (ma + nb) + r$$

which can be written as

$$(1 - qm) a + (-qn) b = r.$$ 

Since $1 - qm$ and $-qn$ are integers and since $r > 0$, we see that $r \in S$. However, we also know that $r < d$ and this is not possible, because $d$ is the smallest member of $S$. Thus, our assumption that $d$ is not a divisor of $a$ has led to a contradiction. We must therefore conclude that $d$ is a divisor of $a$.

For the next step of our proof, we will show that every element of $S$ is an integer of the form $k \cdot \gcd (a, b)$ where $k$ is some positive integer. To this end, let us suppose that $x$ is an element of $S$. Then there exist integers $s$ and $t$ such that $x = sa + tb$ and $x > 0$. Since $\gcd (a, b)$ divides both $a$ and $b$, then $\gcd (a, b)$ must also divide $x$. Therefore, there exists an integer $k$ such that $x = k \cdot \gcd (a, b)$. Since $x > 0$ and $\gcd (a, b) > 0$, then $k$ must also be positive. This proves what we wanted to prove.

3
Finally, we put the pieces together: We have proved that the smallest member of $S$, which is $d$, is a divisor of both $a$ and $b$. We have also proved that every member of $S$ is a number of the form $k \cdot \gcd(a, b)$ where $k$ is some positive integer. This means that $d = k \cdot \gcd(a, b)$ where $k$ is some positive integer. However, this implies that $k = 1$, because no number greater than $\gcd(a, b)$ can be a divisor of both $a$ and $b$. (That would mean that there was a common divisor greater than the greatest common divisor!). In conclusion, $d = \gcd(a, b)$. ■

**Corollary 8** The set $S$ defined above consists precisely of all positive integer multiples of $\gcd(a, b)$. That is,

$$S = \{k \cdot \gcd(a, b) \mid k \in \mathbb{N}\}.$$ 

**Proof.** We have already proved that the smallest member of $S$ is $\gcd(a, b)$. In fact,

$$\gcd(a, b) = ma + nb.$$ 

Multiplying both sides of the above equation by 2 gives

$$2 \cdot \gcd(a, b) = (2m)a + (2n)b.$$ 

Since $2m$ and $2n$ are both integers, we see that $2 \cdot \gcd(a, b) \in S$.

By the same approach, we see that if $k$ is any positive integer, then $k \cdot \gcd(a, b) \in S$.

Furthermore, we know that $S$ contains no numbers other than those of the form $k \cdot \gcd(a, b)$ because this was proved in the proof of the preceding theorem. ■

In order to develop the Euclidean Algorithm, we will need one more Lemma.

**Lemma 9** Suppose that $a$ and $b$ are positive integers and suppose that $q$ and $r$ are the unique integers such that $a = qb + r$ and $0 \leq r < b$ (guaranteed to exist by the Division Algorithm).

1. If $r = 0$ (that is, if $a$ is divisible by $b$), then $\gcd(a, b) = b$.

2. If $r > 0$, then $\gcd(a, b) = \gcd(b, r)$. 

4
Proof. If \( r = 0 \), then \( a = qb \) which means that \( b \) is a divisor of \( a \). It is also clear that \( b \) is a divisor of \( b \) and that \( b \) can have no greater divisor. Therefore \( \gcd (a, b) = b \).

If \( r > 0 \), then since \( a = qb + r \), we see that any common divisor of \( b \) and \( r \) is also a divisor of \( a \) (and \( b \)). Likewise, since \( r = a - qb \), we see that any common divisor of \( a \) and \( b \) is also a divisor of \( r \) (and \( b \)). Therefore the set of common divisors of \( a \) and \( b \) is exactly the same as the set of common divisors of \( b \) and \( r \). This implies that \( \gcd (a, b) = \gcd (b, r) \).

We are now ready to describe the Euclidean Algorithm for computing \( \gcd (a, b) \).

1.1 The Euclidean Algorithm

Given positive integers \( a \) and \( b \), use the Division Algorithm to find the unique integers \( q \) and \( r \) such that

\[
a = qb + r \quad \text{where} \quad 0 \leq r < b.
\]

If \( r = 0 \), then \( \gcd (a, b) = b \) (by Lemma 9) and our problem is solved. If \( r > 0 \), then we know that \( \gcd (a, b) = \gcd (b, r) \) (also by Lemma 9). In this case, we apply the Division Algorithm again to \( b \) and \( r \), finding the unique integers \( q_1 \) and \( r_1 \) such that

\[
b = q_1 r + r_1 \quad \text{where} \quad 0 \leq r_1 < r.
\]

If \( r_1 = 0 \), then \( \gcd (a, b) = \gcd (b, r) = r \) and our problem is solved. If \( r_1 > 0 \), then we know that

\[
\gcd (a, b) = \gcd (b, r) = \gcd (r, r_1)
\]

apply the Division Algorithm again, etc.

We continue applying the Division Algorithm as many times as necessary until we arrive at a remainder of 0. Thus we will have a sequence of equations
that looks like

\[ a = q_0 b + r \quad \text{where} \quad 0 \leq r < b \]
\[ b = q_1 r + r_1 \quad \text{where} \quad 0 \leq r_1 < r \]
\[ r = q_2 r_1 + r_2 \quad \text{where} \quad 0 \leq r_2 < r_1 \]
\[ r_1 = q_3 r_2 + r_3 \quad \text{where} \quad 0 \leq r_3 < r_2 \]
\[ \vdots \]
\[ r_n = q_{n+2} r_{n+1} + r_{n+2} \quad \text{where} \quad 0 \leq r_{n+2} < r_{n+1} \]
\[ r_{n+1} = q_{n+3} r_{n+2} + 0 \]

from which we conclude that

\[ \gcd(a, b) = \gcd(b, r) = \gcd(r, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = \gcd(r_{n+1}, r_{n+2}) = r_{n+2}. \]

This algorithm is best learned by studying some examples and then working some examples on your own.

**Example 10** Use the Euclidean Algorithm to find \( \gcd(48, 60) \).

**Solution 11**

\[
\begin{align*}
60 &= 1(48) + 12 \\
48 &= 4(12) + 0
\end{align*}
\]

Thus

\[ \gcd(60, 48) = \gcd(48, 12) = 12 \]

(because 48 is divisible by 12).

**Example 12** Use the Euclidean Algorithm to find \( \gcd(68, 114) \).

**Solution 13**

\[
\begin{align*}
114 &= 1(68) + 46 \\
68 &= 1(46) + 22 \\
46 &= 2(22) + 2 \\
22 &= 11(2) + 0
\end{align*}
\]

Therefore

\[ \gcd(114, 68) = \gcd(68, 46) = \gcd(46, 22) = \gcd(22, 2) = 2. \]
1.2 Relatively Prime Integers

**Definition 14** Two positive integers, \(a\) and \(b\), are said to be relatively prime if \(\gcd(a, b) = 1\).

**Example 15** 9 and 10 are relatively prime because \(\gcd(9, 10) = 1\).

**Example 16** Use the Euclidean Algorithm to show that 397 and 541 are relatively prime.

**Solution 17**

\[
\begin{align*}
541 &= 1(397) + 144 \\
397 &= 2(144) + 109 \\
144 &= 1(109) + 35 \\
109 &= 3(35) + 4 \\
35 &= 8(4) + 3 \\
4 &= 1(3) + 1 \\
3 &= 3(1) + 0
\end{align*}
\]

shows that \(\gcd(541, 397) = 1\).

The following lemma, called Euclid’s Lemma, is a useful result concerning relatively prime numbers.

**Lemma 18 (Euclid’s Lemma)** If \(a\), \(b\), and \(c\) are positive integers with \(a\) and \(b\) relatively prime and \(a\) divides \(bc\), then \(a\) divides \(c\).

**Proof.** If \(a\) and \(b\) are relatively prime, then \(\gcd(a, b) = 1\). This means that there exist integers \(m\) and \(n\) such that \(1 = ma + nb\).

If \(a\) divides \(bc\), then there exists an integer \(t\) such that \(bc = ta\).

Multiplying both sides of the equation

\[
1 = ma + nb
\]

by \(c\), we obtain

\[
c = mac + nbc = mac + nta = (mc + nt)a
\]

and, since \(mc + nt\) is an integer, we conclude that \(a\) divides \(c\). ■

Another useful result is the following Proposition.
Proposition 19 If $\gcd (a, b) = d$, then $\gcd \left( \frac{a}{d}, \frac{b}{d} \right) = 1$.

Proof. If $\gcd (a, b) = d$, then there are integers $m$ and $n$ such that $ma + nb = d$. Dividing both sides of this equation by $d$, we obtain

$$m \left( \frac{a}{d} \right) + n \left( \frac{b}{d} \right) = 1.$$  

Since $\gcd \left( \frac{a}{d}, \frac{b}{d} \right)$ is the smallest positive integer than can be expressed in the form $s \left( \frac{a}{d} \right) + t \left( \frac{b}{d} \right)$ (where $s$ and $t$ are integers) and since there is no positive integer smaller than 1, we conclude that $\gcd \left( \frac{a}{d}, \frac{b}{d} \right) = 1$. ■

1.3 Least Common Multiples

Definition 20 Let $a$ and $b$ be two integers. The least common multiple of $a$ and $b$, denoted by $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both $a$ and $b$.

Example 21 Find the least common multiple of 15 and 35.

Solution 22 The set of positive multiples of 15 is

$$M(15) = \{15, 30, 45, 60, 75, 90, 105, 120, \ldots \}$$

and the set of positive multiples of 35 is

$$M(35) = \{35, 70, 105, 150, \ldots \}.$$  

Thus we see that $\text{lcm}(15, 35) = 105$.

The following Proposition shows how to find $\text{lcm}(a, b)$ without listing all of the multiples of $a$ and $b$.

Proposition 23 Given two positive integers $a$ and $b$,

$$\text{lcm}(ab) = \frac{ab}{\gcd(a, b)}.$$  

Proof. See proof in textbook. ■

Example 24 By the above Proposition,

$$\text{lcm}(15, 35) = \frac{(15)(35)}{\gcd(15, 35)} = \frac{(15)(35)}{5} = 105.$$  

8
2 Diophantine Equations

A Diophantine equation is an equation of the form

\[ ax + by = c \]

where \( a, b, \) and \( c \) are given integers and \( x \) and \( y \) are the unknowns. Such an equation always has solutions if we allow \( x \) and \( y \) to be real numbers. In fact, the graph of \( ax + by = c \) is a line and any point, \((x, y)\), on this line is a solution. However, we wish to find only pairs \((x, y)\) where \( x \) and \( y \) are both integers.

**Example 25** A solution of the Diophantine equation \( 3x + 12y = 12 \) is \((x, y) = (0,1)\). Another solution is \((4,0)\). Another solution is \((8,-1)\). We will see that any Diophantine equation that has a solution must have infinitely many solutions.

If \( a \) and \( b \) are any integers (not both zero), we know that every expression of the form \( ax + by \), where \( x \) and \( y \) are both integers, must be a multiple of \( \gcd (a, b) \) (by Corollary 8). Therefore the Diophantine equation \( ax + by = c \) has a solution if and only if \( c \) is a multiple of \( \gcd (a, b) \). For example, the Diophantine equation \( 3x + 12y = 15 \) must have solutions because \( \gcd (3, 12) = 3 \) and 15 is a multiple of 3. However, the Diophantine equation \( 3x + 12y = 16 \) does not have any solutions because 16 is not a multiple of 3.

In order to find a solution of the Diophantine equation \( ax + by = c \), we first find a solution of the equation \( ax + by = \gcd (a, b) \) and then, after having found the solution \((x, y)\) of the latter equation, we simply multiply both sides by \( c \) to find a solution of \( ax + by = c \). This procedure is illustrated in the following example.

**Example 26** Find a solution of the Diophantine equation \( 34x + 57y = 3 \).

**Solution 27** First we find \( \gcd (34, 57) \) using the Euclidean Algorithm:

\[
\begin{align*}
57 &= 1(34) + 23 \\
34 &= 1(23) + 11 \\
23 &= 2(11) + 1 \\
11 &= 1(1)
\end{align*}
\]
We see that $\text{gcd}(34, 57) = 1$, and since 3 is a multiple of 1, we know that the equation in question has a solution.

We will now find a solution of the equation $34x + 57y = 1$. To do this, we begin with the 1 (in the box above) and work backwards to eliminate all of the remainders that came up in the Euclidean Algorithm so that 1 is written in terms of 34 and 57. Starting with the third line above, we have

$$1 = 23 - 2 \cdot (11).$$

Substitution of the 11 in the second line gives

$$1 = 23 - 2 \cdot [34 - 1 \cdot (23)].$$

We now simplify to obtain

$$1 = 23 - 2 \cdot (34) + 2 \cdot (23)$$

or

$$1 = 3 \cdot (23) - 2 \cdot (34).$$

Next we substitute the 23 from the first line

$$1 = 3 \cdot [57 - 1 \cdot (34)] - 2 \cdot (34)$$

and simplify to obtain

$$1 = 3 \cdot (57) - 5 \cdot (34).$$

Writing this in the form

$$34 \cdot (-5) + 57 \cdot (3) = 1$$

we see that $(x, y) = (-5, 3)$ is a solution of the equation $34x + 57y = 1$.

Next we multiply both sides of $34 \cdot (-5) + 57 \cdot (3) = 1$ by 3 to obtain

$$34 \cdot (-15) + 57 \cdot (9) = 3,$$

Therefore $(x, y) = (-15, 9)$ is a solution of the equation $34x + 57y = 3$.

Once a solution to a Diophantine equation has been found by the above method, all of the other (infinitely many) solutions of the equation can be found by using the following theorem.
Theorem 28 Suppose that \((x_0, y_0)\) is a solution of the Diophantine equation \(ax + by = c\). Then all solutions of this equation have the form

\[
x = x_0 + \left(\frac{b}{\gcd(a, b)}\right)t
\]
\[
y = y_0 - \left(\frac{a}{\gcd(a, b)}\right)t
\]

where \(t\) can be any integer.

Proof. See proof in textbook. ■

Example 29 In Example 26, we saw that \((x_0, y_0) = (-15, 9)\) is a solution of the Diophantine equation

\[34x + 57y = 3.\]

We also saw that \(\gcd(34, 57) = 1\). Thus all solutions of this equation have the form

\[
x = -15 + \left(\frac{57}{1}\right)t
\]
\[
y = 9 - \left(\frac{34}{1}\right)t.
\]

Thus, for example, if we set \(t = -1\), we obtain the solution \((-72, 43)\). Let’s check to see that this is correct:

\[34(-72) + 57(43) = 3.\]

3 Homework

In Chapter 1, Section 3 (page 25), do problems 1-11.