Greatest Common Divisors and Euclid’s Algorithm

June 2, 2007

1 Greatest Common Divisors

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 \( b \).

For any integer, \( a \), we will use the notation \( D(a) \) to denote the set of all positive divisors of \( a \). With this notation, we can say that

\[
\gcd (a, b) = \max (D(a) \cap D(b)).
\]

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 \( \gcd(48, 60) = 12. \)

**Remark 4** For any integers, \( a \) and \( b, \) the set \( D(a) \cap D(b) \) is not empty because \( 1 \in D(a) \cap D(b) \).

**Remark 5** The reason that \( \gcd(0, 0) \) is not defined is because
\[ D(0) \cap D(0) = D(0) = \{1, 2, 3, 4, \ldots\} \]
and this set has no maximum.

**Example 6** Find the greatest common divisor of 68 and 114.

**Solution 7** 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 \( \gcd(68, 114) = 2. \)

The method by which we found \( \gcd(48, 60) \) and \( \gcd(68, 114) \) 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 (and thus perhaps hard to factor into prime factors), then this method of finding \( \gcd(a, b) \) 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 that \( \gcd(a, b) \) can always be written in the form \( \gcd(a, b) = ma + nb \) where \( m \) and \( n \) are integers. In other words, given any two integers \( a \) and \( b \), there will always exist two integers \( m \) and \( n \) such that \( \gcd(a, b) = ma + nb \). For example, we found that \( \gcd(48, 60) = 12 \) and it is easily seen that

\[
12 = (-1)(48) + (1)(60).
\]

We also found that \( \gcd(68, 114) = 2 \) 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 8** 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 $S$ (according to how we have chosen $d$ in the paragraph preceding this theorem). 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 $a$. (As mentioned, a similar argument also proves that $d$ is a divisor of $b$).

For the next step of our proof, we will show that every element of $S$ is a positive multiple of $\gcd(a, b)$. To this end, let us suppose that $x$ is an arbitrary 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 a positive integer $k$ such that $x = k \cdot \gcd(a, b)$. Since $x$ was originally designated to be an arbitrary member of $S$, we have proved that all members of $S$ are positive multiples of $\gcd(a, b)$.

Finally, we put the pieces together: We have proved that the smallest member of $S$, which we called $d$, is a divisor of both $a$ and $b$. We have also proved that every member of $S$ is an integer 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 9** 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,

$$\gcd(a, b) = ma + nb$$
(where \( m \) and \( n \) are integers). 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 10** 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 \( \gcd(a, b) = \gcd(b, r) \).

**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 10) and our problem is solved. If \( r > 0 \), then we know that \( \gcd(a, b) = \gcd(b, r) \) (also by Lemma 10). 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

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

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

\[
r = q_2 r_1 + r_2 \quad \text{where} \quad 0 \leq r_2 < r_1
\]

\[
r_1 = q_3 r_2 + r_3 \quad \text{where} \quad 0 \leq r_3 < r_2
\]

\[
\vdots
\]

\[
r_n = q_{n+2} r_{n+1} + r_{n+2} \quad \text{where} \quad 0 \leq r_{n+2} < r_{n+1}
\]

\[
r_{n+1} = q_{n+3} r_{n+2} + 0
\]

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

**Solution 12**

\[
60 = 1 (48) + 12
\]

\[
48 = 4 (12) + 0
\]

Thus

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

(because 48 is divisible by 12).
Example 13 Use the Euclidean Algorithm to find gcd (68, 114).

Solution 14

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

Therefore

\[
gcd (114, 68) = gcd (68, 46) = gcd (46, 22) = gcd (22, 2) = 2.
\]

1.2 Relatively Prime Integers

Definition 15 Two positive integers, \(a\) and \(b\), are said to be relatively prime if \(gcd (a, b) = 1\).

Example 16 9 and 10 are relatively prime because \(gcd (9, 10) = 1\).

Example 17 Use the Euclidean Algorithm to show that 397 and 541 are relatively prime.

Solution 18

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

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

The following lemma, called Euclid’s Lemma, is a useful result concerning relatively prime numbers.
Lemma 19 (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 lemma of interest is the following:

Lemma 20 Suppose that \(a\) and \(b\) are integers (not both zero) and suppose that \(d = \gcd(a, b).\) Then \(\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.\)

Proof. Since \(d = \gcd(a, b),\) then there exist integers \(m\) and \(n\) such that

\[
d = ma + nb.
\]

Dividing both sides of the above equation by \(d\) gives us

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

(Note that \(a/d\) and \(b/d\) are both integers because \(a\) and \(b\) are both divisible by \(d.\)) We know that \(\gcd\left(\frac{a}{d}, \frac{b}{d}\right)\) is the smallest positive integer that can be written in the form \(s\left(\frac{a}{d}\right) + t\left(\frac{b}{d}\right)\) when all integer choices of \(s\) and \(t\) are considered. Since the choice \(s = m\) and \(t = n\) gives 1 and since 1 is the smallest positive integer, it must be true that \(\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.\)

1.3 Least Common Multiples

Definition 21 Let \(a\) and \(b\) be two non-zero 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 \(b.\)
For any integer, \( a \), we will use the notation \( M(a) \) to denote the set of all positive multiples of \( a \). With this notation, we can say that 
\[
lcm(a, b) = \min(M(a) \cap M(b)).
\]

**Example 22** Find the least common multiple of 15 and 35.

**Solution 23** 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 \( \text{lcm}(15, 35) = 105 \).

**Exercise 24** Is it possible to find two positive integers, \( a \) and \( b \), such that \( M(a) \cap M(b) = \emptyset \)? Why or why not?

### 2 Some Relationships Between \( \gcd \) and \( \text{lcm} \)

Although the Euclidean Algorithm can always be used to find \( \gcd(a, b) \), it is not necessary to use this algorithm in cases where the numbers \( a \) and \( b \) can be easily factored. In such cases, the following result can be used to find both \( \gcd(a, b) \) and \( \text{lcm}(a, b) \).

**Theorem 25** Suppose that \( a \) and \( b \) are positive integers and suppose that 
\[
\frac{b}{a} = \frac{s}{t}
\]
where \( s \) and \( t \) are positive integers with \( \gcd(s, t) = 1 \). Then 
\[
\gcd(a, b) = \frac{a}{t} = \frac{b}{s}
\]
and 
\[
\text{lcm}(a, b) = sa = tb.
\]
Proof. Since we are starting with the assumption that
\[
\frac{b}{a} = \frac{s}{t},
\]
then it is easy to see that both
\[
\frac{a}{t} = \frac{b}{s} \quad \text{and} \quad sa = tb
\]
must be true. Since \(a, b, s,\) and \(t\) are all integers, it is clear that \(sa\) and \(tb\) are also integers. We need to make sure that \(a/t\) and \(b/s\) are also integers. To see why this must be true, note that since \(sa = tb\) and \(s\) divides \(sa\), then \(s\) also divides \(tb\). However, since \(s\) and \(t\) are relatively prime (by assumption), Euclid’s Lemma allows us to conclude that \(s\) divides \(b\). Therefore \(b/s\) is an integer. Since \(a/t = b/s\), then \(a/t\) is also obviously (the same) integer.

Let 
\[
d = \frac{a}{t} = \frac{b}{s}
\]
and
\[
m = sa = tb.
\]
We want to prove that \(d = \gcd(a, b)\) and \(m = \text{lcm}(a, b)\).

Since \(a = td\) and \(b = sd\), we can see that \(d\) is a common divisor of \(a\) and \(b\). We need to show that if \(D\) is any positive common divisor of \(a\) and \(b\), then \(D \leq d\). To this end, suppose that \(D\) is a positive common divisor of \(a\) and \(b\). Then there exist integers \(p\) and \(q\) such that
\[
a = pD \quad \text{and} \quad b = qD.
\]
From this we obtain that \(\frac{b}{a} = \frac{q}{p}\). However, we also know that \(\frac{b}{a} = \frac{s}{t}\) and thus \(\frac{b}{a} = \frac{q}{p}\) and \(ps = qt\). Since \(s\) divides \(ps\), then \(s\) divides \(qt\). However \(s\) and \(t\) are relatively prime, so Euclid’s Lemma allows us to conclude that \(s\) divides \(q\). By similar reasoning, we can conclude that \(t\) divides \(p\). Thus there are positive integers \(x\) and \(y\) such that \(q = xs\) and \(p = yt\). This gives us
\[
a = ytD \quad \text{and} \quad b = xsD.
\]
We now have
\[
_td = y_D \quad \text{and} \quad sd = xsD
\]
which gives us
\[ d = yD \quad \text{and} \quad d = xD \]
and we conclude that
\[ \frac{d}{D} = \frac{y}{x}. \]
However, since \( x \) is a positive integer, then \( x \geq 1 \). Thus \( d \geq D \). This proves that any common divisor of \( a \) and \( b \) must be less than or equal to \( d \). Therefore \( d = \gcd(a, b) \).

Next we show that \( m = \lcm(a, b) \). (The proof is similar to the above proof that \( d = \gcd(a, b) \) and some of the same notation used in that proof will be recycled.) Since \( m = sa = tb \), then \( m \) is a common multiple of \( a \) and \( b \). Now suppose that \( M \) is any positive common multiple of \( a \) and \( b \). Then there exist integers \( p \) and \( q \) such that \( M = pa \) and \( M = qb \). This gives us
\[ sM = spa = pm \quad \text{and} \quad tM = tqb = qm. \]
Thus
\[ \frac{M}{m} = \frac{p}{s} = \frac{q}{t} \]
and hence \( pt = qs \). Since \( s \) and \( t \) are relatively prime, Euclid’s Lemma allows us to conclude that \( t \) divides \( q \) and \( s \) divides \( p \). Thus there are positive integers \( x \) and \( y \) such that \( q = tx \) and \( p = sy \). This gives us
\[ \frac{M}{m} = \frac{y}{x}. \]
Since \( x \) is a positive integer, then \( x \geq 1 \) and we conclude that \( M \geq m \). We have now shown that any positive common multiple of \( a \) and \( b \) must be greater than or equal to \( m \). Therefore \( m = \lcm(a, b) \).

**Example 26** Use Theorem 25 to find \( \gcd(48, 60) \) and \( \lcm(48, 60) \).

**Solution 27** In order to use the theorem, we need to write 60/48 in lowest terms:
\[ \frac{60}{48} = \frac{5}{4}. \]
Since \( \gcd(5, 4) = 1 \), Theorem 25 allows us to conclude that
\[ \gcd(48, 60) = \frac{48}{4} = \frac{60}{5} = 12 \]
and
\[ \lcm(48, 60) = 5(48) = 4(60) = 240. \]
Exercise 28  Use Theorem 25 to find $\gcd(68, 114)$ and $\text{lcm}(68, 114)$.

We now give two corollaries of Theorem 25.

Corollary 29  Suppose that $a$ and $b$ are any two positive integers. Then

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

Proof. When we write $b/a$ in lowest terms, we obtain $b/a = s/t$ where $s$ and $t$ are relatively prime. Theorem 25 then tells us that $\gcd(a, b) = b/s$ and $\text{lcm}(a, b) = sa$. Thus

$$\gcd(a, b) \cdot \text{lcm}(a, b) = \left(\frac{b}{s}\right)(sa) = ab.$$  

Corollary 30  Suppose that $a$ and $b$ are positive integers. Then $\gcd(a, b) = 1$ if and only if $\text{lcm}(a, b) = ab$.

Proof. Using the above corollary, we see that $\gcd(a, b) = 1$ if and only if

$$1 \cdot \text{lcm}(a, b) = ab.$$  

3  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. When we say that we are going to “solve the Diophantine equation $ax + by = c$”, we mean that we are going to find all integer pairs, $(x, y)$, that satisfy the equation.
Example 31 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), then we know that the Diophantine equation

$$ax + by = \gcd (a, b)$$

has a solution. This is because we know that there must exist an integer pair, $(m, n)$, such that

$$am + bn = \gcd (a, b).$$

Furthermore, we know that the only integers that can be written in the form $ax + by$ (where $x$ and $y$ are both integers) are multiples of $\gcd (a, b)$ (by Corollary 9). 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 $k$ (where $c = k \cdot \gcd (a, b)$) to find a solution of $ax + by = c$. This procedure is illustrated in the following example.

Example 32 Find a solution of the Diophantine equation $34x + 57y = 3$.

Solution 33 First we find $\gcd (34, 57)$ using the Euclidean Algorithm:

$$57 = 1(34) + 23$$
$$34 = 1(23) + 11$$
$$23 = 2(11) + 1$$
$$11 = 11(1).$$

We see that $\gcd (34, 57) = 1$, 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 34** Suppose that \((x_0, y_0)\) is a solution of the Diophantine equation \(ax + by = c\) and suppose that \(d = \gcd(a, b)\). Then all solutions of this equation have the form

\[ x = x_0 + \frac{tb}{d} \]
\[ y = y_0 - \frac{ta}{d} \]

where \(t\) can be any integer.

14
Proof. Suppose that \( x_0, y_0, x, \) and \( y \) are integers such that \( ax_0 + by_0 = c \) and \( ax + by = c \). Let \( d = \gcd(a, b) \).

Since \( a, b, \) and \( c \) are all divisible by \( d \), we obtain

\[
\left( \frac{a}{d} \right) x_0 + \left( \frac{b}{d} \right) y_0 = \frac{c}{d}
\]

and

\[
\left( \frac{a}{d} \right) x + \left( \frac{b}{d} \right) y = \frac{c}{d}.
\]

By subtracting, we obtain

\[
\left( \frac{a}{d} \right) (x - x_0) + \left( \frac{b}{d} \right) (y - y_0) = 0
\]

which gives us

\[
y - y_0 = -\frac{a}{b} \left( x - x_0 \right) .
\]

Now let \( x - x_0 = p \) and \( y - y_0 = q \). Then \( p \) and \( q \) are both integers and

\[
q = -\frac{a}{b} p.
\]

By Lemma 20, we know that \( \gcd\left( \frac{a}{d}, \frac{b}{d} \right) = 1 \). Since \( q \) is an integer, it must thus be the case that \( p \) is divisible by \( \frac{b}{d} \). Therefore there exists an integer \( t \) such that \( p = \frac{tb}{d} \) and we obtain

\[
q = -\frac{ta}{d}.
\]

We have now shown that all solutions of the Diophantine equation \( ax + by = c \) must have the form

\[
x = x_0 + \frac{tb}{d}
\]

\[
y = y_0 - \frac{ta}{d}
\]

where \( t \) is some integer and \( (x_0, y_0) \) is a known solution of \( ax + by = c \). In order to complete the proof of this theorem, we must show that any integer
choice of $t$ works. To this end, let $t$ be any integer and let $x$ and $y$ be defined as above. Then

$$ax + by = a \left( x_0 + \frac{tb}{d} \right) + b \left( y_0 - \frac{ta}{d} \right)$$

$$= ax_0 + by_0$$

$$= c.$$ 

This completes the proof of the theorem. ■

**Example 35** In Example 32, 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

$$x = -15 + \frac{57t}{1}$$

$$y = 9 - \frac{34t}{1}.$$ 

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

$$34(-72) + 57(43) = 3.$$ 

4 **Homework**

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