Greatest Common Divisors

DEFINITION: A **common divisor** of two integers a and b, which are not both 0, is an integer c such that $c \mid a$ and $c \mid b$. The **greatest common divisor** (gcd) of a and b, denoted by (a, b), is the largest common divisor of integers a and b.

DEFINITION: The integers a and b, with $a \neq 0$ and $b \neq 0$, are **relatively prime** if

$$(a, b) = 1$$

THEOREM 1: Let a, b, and c be integers with $(a, b) = d$. Then

(i) $(a/d, b/d) = 1$ (ii) $(a + cb, b) = (a, b)$

EXAMPLE: Let a be an integer number. Show that

(a) $(2a + 3, a + 2) = 1$ (b) $(7a + 2, 10a + 3) = 1$

Solution: By the Theorem above we have

$$\begin{aligned}(2a+3, a+2) &= (a+1+a+2, a+2)\\ &= (a+1, a+2)\\ &= (a+1, a+1+1)\\ &= (a+1, 1)\\ &= 1\end{aligned}$$

$$\begin{aligned}(7k+2,\ 10k+3) &= (7k+2,\ 7k+2+3k+1)\\ &= (7k+2,\ 3k+1)\\ &= (6k+2+k,\ 3k+1)\\ &= (k,\ 3k+1)\\ &= (k,\ 1)\\ &= 1\end{aligned}$$

DEFINITION: If a and b are integers, then a **linear combination** of a and b is a sum of the form $ma + nb$, where both m and n are integers.

THEOREM 2: The greatest common divisor of the integers a and b, that are not both zero, is the least positive integer that is a linear combination of a and b.

Proof: Let d be the least positive integer that is a linear combination of a and b. We write

$$d = sa + tb \tag{1}$$

where s and t are integers. We first show that $d \mid a$. By the Division Algorithm we have

$$a = dq + r, \text{ where } 0 \leq r < d$$

From this and (1) it follows that

$$r = a - dq = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b$$

This shows that r is a linear combination of a and b. Since $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d is a common divisor of a and b. We now show that d is the *greatest common divisor* of a and b. Assume to the contrary that $(a, b) = d'$ and $d' > d$. Since $d' \mid a$, $d' \mid b$ and $d = sa + tb$, it follows that $d' \mid d$ by Theorem 2 from Section 1.5, therefore $d' \leq d$. We obtain a contradiction. So, d is the greatest common divisor of a and b and this concludes the proof. ■

COROLLARY 1 (BEZOUT'S THEOREM): If a and b are integers, then there are integers m and n such that

$$ma + nb = (a, b)$$

EXAMPLE: Note that $(4, 10) = 2$. Since $2 = 10 - 4 \cdot 2$, it follows that

$$(-2) \cdot 4 + 1 \cdot 10 = (4, 10)$$

In fact, there are infinitely many numbers m and n such that

$$4m + 10n = (4, 10) \tag{2}$$

because $m = -2 + 10t$ and $n = 1 - 4t$ satisfy (2) for any t.

EXAMPLE: Show that the equation

$$56x + 105y = 7 \tag{3}$$

has a solution in integer numbers.

Solution: One can check that $(56, 105) = 7$, therefore (3) has a solution in integer numbers by Corollary 1. Moreover, (3) has infinitely many solutions in integer numbers, because $x = -13 - 15t$ and $y = 7 + 8t$ satisfy (3) for any t.

COROLLARY 2: The integers a and b are relatively prime integers if and only if there are integers m and n such that

$$ma + nb = 1$$

Proof: The prove this corollary, note that if a and b are relatively prime, then $(a, b) = 1$. Consequently, by the Theorem above, 1 is the least positive integer that is a linear combination of a and b. It follows that there are integers m and n such that $ma + nb = 1$.

Conversely, if there are integers m and n with $ma + nb = 1$, then by the Theorem above, it immediately follows that $(a, b) = 1$. This follows because not both a and b are zero and 1 is clearly the least positive integer that is a linear combination of a and b. ■

THEOREM 3: If a and b are positive integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).

Proof: Suppose that $d = (a, b)$. We first show that every linear combination of a and b must also be a multiple of d. First note that by the definition of greatest common divisor, we know that $d \mid a$ and $d \mid b$. Now every linear combination of a and b is of the form $ma + nb$, where m and n are integers. By Theorem 2 from Section 1.5, it follows that whenever m and n are integers, d divides $ma + nb$. That is, $ma + nb$ is a multiple of d.

We now show that every multiple of d is also a linear combination of a and b. By the Theorem above, we know that there are integers r and s such that

$$(a, b) = ra + sb$$

The multiples of d are the integers of the form jd, where j is an integer. Multiplying both sides of the equation $d = ra + sb$ by j, we see that

$$jd = (jr)a + (js)b$$

Consequently, every multiple of d is a linear combination of a and b. ■

THEOREM 4: If a and b are integers, not both 0, then a positive integer d is the greatest common divisor of a and b if and only if

(a) $d \mid a$ and $d \mid b$, and

(b) if c is an integer with $c \mid a$ and $c \mid b$, then $c \mid d$

DEFINITION: Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. The **greatest common divisor** of these integers is the largest integer which is a divisor of all of the integers in the set. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$.

EXAMPLE: We easily see that $(12, 18, 30) = 6$ and $(10, 15, 25) = 5$.

To find the greatest common divisor of a set of more than two integers, we can use the following lemma.

LEMMA: If $a_1, a_2, \ldots, a_n$ are integers, not all zero, then

$$(a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$$

EXAMPLE: To find the greatest common divisor of the three integers 105, 140, and 350, we use the Lemma above to see that

$$(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35$$

DEFINITION: We say that the integers $a_1, a_2, \ldots, a_n$ are **mutually relatively prime** if $(a_1, a_2, \ldots, a_n) = 1$. These integers are called **pairwise relatively prime** if for each pair of integers a_i and a_j with $i \neq j$ from the set, $(a_i, a_j) = 1$; that is, if each pair of integers from the set is relatively prime.

It is easy to see that if integers are pairwise relatively prime, they must be mutually relatively prime. However, the converse is false as the following example shows.

EXAMPLE: Consider the integers 15, 21, and 35. Since

$$(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1$$

we see that the three integers are mutually relatively prime. However, they are not pairwise relatively prime, because

$$(15, 21) = 3, \quad (15, 35) = 5, \quad \text{and} \quad (21, 35) = 7$$