

7. Greatest Common Divisors, Least Common Multiples

We have met the concept of the greatest common divisor of two integers. We now look at a closely related idea.

Definition

For integers a, b an integer c is a common multiple of a, b if $a \mid c$ and $b \mid c$.

As 0 is a multiple of *any* integer, it is a common multiple for *any* pair a, b .

For any a, b , ab and $-ab$ are obvious common multiples of a and b . If a and b are non-zero, then *one* of these products is positive. This leads us to the

Definition

For non-zero integers a, b , the *least common multiple* of a, b is the least positive integer which is a common multiple of a, b . It is denoted by $\text{lcm}(a, b)$.

We observe that $\text{lcm}(a, b)$ is the integer m such that

- $a \mid m$ and $b \mid m$
- if $c > 0$ has $a \mid c$ and $b \mid c$, then $m \leq c$.

The first condition states that m is a common multiple. The second guarantees that it is *the least positive* common multiple.

For example, $\text{lcm}(12, 30) = 60$. To see this, look at the positive multiples of 30. These are 30, 60, ... The lcm is the smallest which is also a multiple of 12, i.e. 60.

Theorem 1

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

Proof

Put $d = \text{gcd}(a, b)$. Then we have *integers* u, v with $a = du$, $b = dv$, and $\text{gcd}(u, v) = 1$

Put $m = duv$. We will show that this is $\text{lcm}(a, b)$.

As $du = a$, $m = av$, so $a \mid m$.

As $dv = b$, $m = ub$, so $b \mid m$.

Thus m is a common multiple. It is positive as d, u, v are positive.

Now suppose that c is *any* positive common multiple of a and b .

As c is a common multiple, $b \mid c$, so $c = kb$ for some integer k .

We also have $a \mid c$, so $c = ra$ for some integer r

But $c = kb$, so $kb = ra$, i.e. $kdv = rdu$.

Cancelling the factor d , .

Then $u \mid kv$. As $\text{gcd}(u, v) = 1$, Euclid's lemma shows that $u \mid k$.

Thus $k = us$ for some positive integer s .

Then $c = kb = (us)(dv) = (duv)s = ms$.

As $s \geq 1$, $c \geq m$.

Thus, $m = \text{lcm}(a, b)$.

Finally, $\text{gcd}(a, b) \cdot \text{lcm}(a, b) = dm = d(duv) = (du)(dv) = ab$, as required.

This gives a more efficient way of finding $\text{lcm}(a,b)$ for non-zero integers a, b . We can use the Euclidean Algorithm to find $\text{gcd}(a,b)$. This is very quick. We can then determine $\text{lcm}(a,b)$ as $ab/\text{gcd}(a,b)$. For example, it is easy to verify that $\text{gcd}(12,30) = 6$, so $\text{lcm}(12,30) = 12 \cdot 30 / 6 = 60$.

We can extend the ideas of greatest common divisor and least common multiple to lists of more than two integers in a fairly obvious way. For example

If a, b, c are integers, but not all zero, then the greatest common divisor of a, b, c is the positive integer d satisfying

- $d \mid a, d \mid b, d \mid c$,
- if e is any integer with $e \mid a, e \mid b, e \mid c$, then $e \leq d$.

It is denoted by $\text{gcd}(a,b,c)$.

There is no need to develop a new body of theory to deal with this generalization since we have the following results. We omit the proofs.

Theorem 2

If a, b, c are integers, no two of which are zero, then $\text{gcd}(a,b,c) = \text{gcd}(a,\text{gcd}(b,c))$.

Theorem 3

If a, b, c are non-zero integers, then $\text{lcm}(a,b,c) = \text{lcm}(a, \text{lcm}(b,c))$.

Thus, the theory for the gcd and lcm of *two* integers gives results for three (or even more).

Example Find $\text{gcd}(777, 2675, 4655)$.

Solution

By Theorem 2, $\text{gcd}(777, 2675, 4655) = \text{gcd}(777, \text{gcd}(2675, 4655))$

From an earlier example, $\text{gcd}(2675, 4655) = 35$.

Thus, the answer is given by $\text{gcd}(777,35)$. We can find this in the usual way :

$$777 = 22 \cdot 35 + 7$$

$$35 = 5 \cdot 7 + 0$$

Thus, $\text{gcd}(777, 35) = 7$, so $\text{gcd}(777, 2675, 4655) = 7$.

These results also allow us to investigate linear diophantine equations in more than two variables. For example, again stated without proof ;

Theorem 4 Suppose that a, b, c are non-zero integers. Let $d = \text{gcd}(a,b,c)$. The diophantine equation $ax+by+cz = e$ has integral solutions if and only if $d \mid e$.

Solving a diophantine equation in more than two variables can be achieved by using the two-variable method a number of times.

Consider the equation

$$ax+by+cz = d, \quad (1)$$

where a, b, c, d are integers, with a, b, c non-zero.

Let $f = \gcd(b,c)$, and $e = \gcd(a,b,c)$.

By Theorem 2, $e = \gcd(a,f)$.

By Theorem 4, there are solutions provided $e \mid d$.

As $e \mid d$, we can find integers such that

$$aX+fW = d \quad (2)$$

As $f = \gcd(b,c)$, we can find integers Y, Z such that

$$bY+cZ = f.$$

Substituting $bY+cZ$ for f in (2), we get

$$aX+bYW+cZW = d.$$

Thus, we have an integral solution of (1), $x = X, y = YW, z = ZW$.

Example Find an integral solution of the equation $91x+126y+294z = 21$.

Solution Following the above strategy, we begin by finding $\gcd(126,294)$.

$$\begin{aligned} 294 &= 2 \cdot 126 + 42 \\ 126 &= 3 \cdot 42 + 0 \end{aligned}$$

Thus, $\gcd(126,294) = 42$.

Backtracking in the first line), we see that

$$42 = 1 \cdot 294 - 2 \cdot 126. \quad (1)$$

From Theorem 2, we know that $\gcd(91,126,294) = \gcd(91,\gcd(126,294))$, and that this is $\gcd(91,42)$. We determine this last.

$$\begin{aligned} 91 &= 2 \cdot 42 + 7 \\ 42 &= 6 \cdot 7 + 0 \end{aligned}$$

Backtracking, we see that

$$7 = 1 \cdot 91 - 2 \cdot 42. \quad (2)$$

As in the strategy, we now find an integral solution of the equation

$$91X + 42W = 21. \quad (3)$$

As $\gcd(91,42) = 7 \mid 21$, there are integral solutions. As $21 = 3 \cdot 7$, and using (2), we have

$$21 = 3 \cdot 7 = 3 \cdot (1 \cdot 91 - 2 \cdot 42)$$

$$= 3 \cdot 91 - 6 \cdot 42$$

$$= 3 \cdot 91 - 6 \cdot (1 \cdot 294 - 2 \cdot 126) \quad \text{using (1)}$$

$$= 3 \cdot 91 - 6 \cdot 294 + 12 \cdot 126$$

Thus, we have the integral solution $x = 3, y = 12, z = -6$.