ADVANCED HIGHER MATHEMATICS

THE EUCLIDEAN ALGORITHM

The **greatest common divisor** (gcd) of two integers a and b is the largest integer which divides into both a and b exactly without remainder. The notation (a, b) is sometimes used to denote the greatest common divisor of a and b. The greatest common divisor of a and b is also known as the **highest common factor** (hcf) of a and b.

Example

Find the greatest common divisor of 12 and 30.

Divisors of 12: 1, 2, 3, 4, 6, 12

Divisors of 30: 1, 2, 3, 5, 6, 10, 15, 30

The greatest common divisor of 12 and 30 is 6.
We write $(12, 30) = 6$.

It is impractical to find the greatest common divisor of a and b by listing divisors when a and b are large. The Euclidean algorithm can instead be used to find the greatest common divisor of a and b.

The following examples illustrate the application of the Euclidean algorithm.

Worked Example 1

Find the greatest common divisor of 140 and 252.

Solution

First express the larger number (252) in terms of the smaller number (140):

$$252 = 1 \times 140 + 112$$

Now express 140 in terms of 112:

$$140 = 1 \times 112 + 28$$

Now express 112 in terms of 28:

$$112 = 4 \times 28 + 0$$

The remainder is now zero and the greatest common divisor is the last non-zero remainder.
Hence $(140, 252) = 28$.

Worked Example 2

Use the Euclidean algorithm to find the greatest common divisor of 132 and 424.

Solution

First express 424 in terms of 132:

$$424 = 3 \times 132 + 28$$

Now express 132 in terms of 28:

$$132 = 4 \times 28 + 20$$

Now express 28 in terms of 20:

$$28 = 1 \times 20 + 8$$

Now express 20 in terms of 8:

$$20 = 2 \times 8 + 4$$

Now express 8 in terms of 4:

$$8 = 2 \times 4 + 0$$

The remainder is now zero and the greatest common divisor is 4.
Hence $(132, 424) = 4$.

Worked Example 3

Use the Euclidean algorithm to find the greatest common divisor of 280 and 117.

Solution

First express 280 in terms of 117:

$$280 = 2 \times 117 + 46$$

Now express 117 in terms of 46:

$$117 = 2 \times 46 + 25$$

Now express 46 in terms of 25:

$$46 = 1 \times 25 + 21$$

Now express 25 in terms of 21:

$$25 = 1 \times 21 + 4$$

Now express 21 in terms of 4:

$$21 = 5 \times 4 + 1$$

Now express 4 in terms of 1:

$$4 = 4 \times 1 + 0$$

The remainder is now zero and the greatest common divisor is 1.
Hence (280, 117) = 1.

[*Note: If $(a, b) = 1$, the integers a and b are said to be* ***co-prime*** *or* ***relatively prime.***]

The Euclidean algorithm can also be used to express the greatest common divisor of integers a and b as a **linear combination** of a and b.

That is, we can find integers x and y such that $(a, b) = xa + yb$.

Worked Example 4

Use the Euclidean algorithm to show that $(149, 139) = 1$.
Hence find integers x and y such that $149x + 139y = 1$.

Solution

First express 149 in terms of 139:

$$149 = 1 \times 139 + 10 \qquad ...(1)$$

Now express 139 in terms of 10:

$$139 = 13 \times 10 + 9 \qquad ...(2)$$

Now express 10 in terms of 9:

$$10 = 1 \times 9 + 1 \qquad ...(3)$$

Now express 9 in terms of 1:

$$9 = 9 \times 1 + 0 \qquad ...(4)$$

The remainder is now zero and the greatest common divisor is 1.
Hence $(149, 139) = 1$.

To express the greatest common divisor as a linear combination of 149 and 139, repeatedly substitute expressions for the remainders in lines (3), (2) and (1).

From line (3): $1 = 10 - 1 \times 9$

Using line (2):
$$\begin{aligned} 1 &= 10 - 1 \times (139 - 13 \times 10) \\ &= 10 - 1 \times 139 + 13 \times 10 \\ &= 14 \times 10 - 1 \times 139 \end{aligned}$$

Using line (1):
$$\begin{aligned} 1 &= 14 \times (149 - 1 \times 139) - 1 \times 139 \\ &= 14 \times 149 - 14 \times 139 - 1 \times 139 \\ &= 14 \times 149 - 15 \times 139 \end{aligned}$$

Hence $149 \times 14 + 139 \times (-15) = 1$.

Thus $149x + 139y = 1$ where $x = 14$ and $y = -15$.

Worked Example 5

Use the Euclidean algorithm to show that $(231, 17) = 1$.
Hence find integers x and y such that $231x + 17y = 1$.

Solution

First express 231 in terms of 17:

$$231 = 13 \times 17 + 10 \quad \ldots(1)$$

Now express 17 in terms of 10:

$$17 = 1 \times 10 + 7 \quad \ldots(2)$$

Now express 10 in terms of 7:

$$10 = 1 \times 7 + 3 \quad \ldots(3)$$

Now express 7 in terms of 3:

$$7 = 2 \times 3 + 1 \quad \ldots(4)$$

Now express 3 in terms of 1:

$$3 = 3 \times 1 + 0 \quad \ldots(5)$$

The remainder is now zero and the greatest common divisor is 1.
Hence $(231, 17) = 1$.

From line (4): $1 = 7 - 2 \times 3$

Using line (3):

$$\begin{aligned} 1 &= 7 - 2 \times (10 - 1 \times 7) \\ &= 7 - 2 \times 10 + 2 \times 7 \\ &= 3 \times 7 - 2 \times 10 \end{aligned}$$

Using line (2):

$$\begin{aligned} 1 &= 3 \times (17 - 1 \times 10) - 2 \times 10 \\ &= 3 \times 17 - 3 \times 10 - 2 \times 10 \\ &= 3 \times 17 - 5 \times 10 \end{aligned}$$

Using line (1):

$$\begin{aligned} 1 &= 3 \times 17 - 5 \times (231 - 13 \times 17) \\ &= 3 \times 17 - 5 \times 231 + 65 \times 17 \\ &= 68 \times 17 - 5 \times 231 \end{aligned}$$

Hence $231 \times (-5) + 17 \times 68 = 1$.

Thus $231x + 17y = 1$ where $x = -5$ and $y = 68$.