Further Number Theory

The Division Algorithm

203 ÷ 25 = 8 rem 3 => 203 = 8 × 25 + 3

If $a, b \in Z^+$, then $\exists$ a unique $q, r \in$ non-negative Z such that $a = bq + r$ where $0 \leq r < b$

Example

a = 193, b = 17

193 ÷ 17 = 11 rem 6 => 193 = 11 × 17 + 6

Exercise

Use the division algorithm for the following

1. a = 75 b = 12
2. a = 327 b = 13
3. a = 392 b = 19

If $r = 0$ then we say that b is a divisor of a.

The greatest common divisor (g.c.d) of a and b is denoted by (a, b)

e.g. (15, 24) = 3

The Euclidean Algorithm

This is used to find the g.c.d of two integers where it cannot be found simply.

It involves repeated use of the division algorithm until $r = 0$.

Example

Find the g.c.d of:

1. 15 and 24
2. 1147 and 851

1.

$$24 = 1 \times 15 + 9$$
$$15 = 1 \times 9 + 6$$
$$9 = 1 \times 6 + 3$$
$$6 = 2 \times 3 + 0$$

Hence (24, 15) = 3

1.

$$1147 = 1 \times 851 + 296$$
$$851 = 2 \times 296 + 259$$
$$296 = 1 \times 259 + 37$$
$$259 = 7 \times 37 + 0$$

Hence (1147, 851) = 37

Exercise

Find the g.c.d of:

1. (a) (15, 27) 3 (b) (16, 42) 2 (c) (72, 108) 36
2. (a) (1219, 901) 53 (b) (2821, 4277) 91 (c) (5213, 2867) 1

Expressing $d = (a, b)$ in the form $d = ax + by$

Example

Express

(a) (24, 15) in the form $24x + 15y$

(b) (1147, 851) in the form $1147x + 851y$

(a)

$$24 = 1 \times 15 + 9 \quad (1)$$
$$15 = 1 \times 9 + 6 \quad (2)$$
$$9 = 1 \times 6 + 3 \quad (3)$$
$$6 = 2 \times 3 + 0$$

=> (24, 15) = 3

$$= 9 - 1(6)$$
$$= 9 - 1(15 - 1(9))$$
$$= 2(9) - 15$$
$$= 2(24 - 1(15)) - 15$$
$$= 2(24) - 3(15)$$

(b)

$$1147 = 1 \times 851 + 296 \quad (1)$$
$$851 = 2 \times 296 + 259 \quad (2)$$
$$296 = 1 \times 259 + 37 \quad (3)$$
$$259 = 7 \times 37 + 0$$

=> (1147, 851) = 37

$$= 296 - 1(259)$$
$$= 296 - 1(851 - 2(296))$$
$$= 3(296) - 851$$
$$= 3(1147 - 1(851)) - 851$$
$$= 3(1147) - 4(851)$$

Use the Euclidean Algorithm to find integers x and y such that

$$83x + 239y = 1.$$

$$239 = 2 \times 83 + 73 \qquad \mathbf{1}$$
$$83 = 1 \times 73 + 10$$
$$10 = 3 \times 3 + 1 \qquad \mathbf{1}$$

Thus

$$1 = 10 - 3(73 - 7 \times 10) \qquad \mathbf{1}$$
$$= 22 \times 10 - 3 \times 73$$
$$= 22(83 - 73) - 3 \times 73$$
$$= 22 \times 83 - 25(239 - 2 \times 83)$$
$$= 72 \times 83 - 25 \times 239 \qquad \mathbf{1}$$

Use the Euclidean algorithm to find integers x, y such that

$$29x + 113y = 1.$$

$$113 = 3 \times 29 + 26 \qquad \mathbf{1}$$
$$29 = 1 \times 26 + 3$$
$$26 = 8 \times 3 + 2$$
$$3 = 1 \times 2 + 1 \qquad \mathbf{1}$$

So

$$1 = 3 - 1 \times (26 - 8 \times 3) = 9 \times 3 - 1 \times 26 \qquad \mathbf{1}$$
$$= 9(29 - 26) - 26 = 9 \times 29 - 10 \times 26$$
$$= 9 \times 29 - 10(113 - 3 \times 29)$$
$$= 39 \times 29 - 10 \times 113 \qquad \mathbf{1}$$

So $x = 39$, $y = -10$ satisfy request.

Use the Euclidean algorithm to show that $(231, 17) = 1$ where (a, b) denotes the highest common factor of a and b.
Hence find integers x and y such that $231x + 17y = 1$.

$$231 = 13 \times 17 + 10$$ **1 for method**
$$17 = 1 \times 10 + 7$$
$$10 = 1 \times 7 + 3$$
$$7 = 2 \times 3 + 1$$ **1**

Thus the highest common factor is 1.

$$1 = 7 - 2 \times 3$$
$$= 7 - 2 \times (10 - 7) = 3 \times 7 - 2 \times 10$$ **1 for method**
$$= 3 \times (17 - 10) - 2 \times 10 = 3 \times 17 - 5 \times 10$$
$$= 3 \times 17 - 5 \times (231 - 13 \times 17) = 68 \times 17 - 5 \times 231.$$ **1**

So $x = -5$ and $y = 68$.