28 / 2 / 18

Number Theory - Lesson 1

The Euclidean Algorithm and the GCD

LI

- Know the Division and Euclidean Algorithms.
- Use the Euclidean Algorithm to find the GCD of two numbers.
- Express the GCD of two numbers in the form $ax + by$.
- Determine whether or not two numbers are coprime.

SC

- Division with remainders.

Jan 10-12:11

The **Division Algorithm** states that, given $a, b \in \mathbb{N}$, $\exists$ unique $q, r \in \mathbb{N}$ satisfying,

$$a = \underbrace{b\,q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}} \quad (0 \leq r < b)$$

The **greatest common divisor (GCD)** (aka **highest common factor (HCF)**) of $a, b \in \mathbb{N}$ - denoted by $GCD(a, b)$ or just (a, b) - is the biggest natural number that exactly divides both a and b

When $a = b\,q + r \ (0 \leq r < b)$, $(a, b) = (b, r)$

Note that $(p, 0) = p$, for any $p \in \mathbb{N}$

Note that $(p, 1) = 1$, for any $p \in \mathbb{N}$

Repeated use of the the Division Algorithm gives the Euclidean Algorithm to work out (a, b) :

$$a = b\,q_1 + r_1 \qquad (0 \le r_1 < b) \qquad (a, b) = (b, r_1)$$

$$b = r_1\,q_2 + r_2 \qquad (0 \le r_2 < r_1) \qquad (b, r_1) = (r_1, r_2)$$

$$r_1 = r_2\,q_3 + r_3 \qquad (0 \le r_3 < r_2) \qquad (r_1, r_2) = (r_2, r_3)$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$r_{k-2} = r_{k-1}\,q_k + 0 \qquad (0 < r_{k-1}) \qquad (r_{k-2}, r_{k-1}) = (r_{k-1}, 0)$$

Then $(a, b) = r_{k-1}$

For any $a, b \in \mathbb{N}$, the Euclidean algorithm can be used to write (a, b) as,

$$(a, b) = a\,x + b\,y \quad (x, y \in \mathbb{Z})$$

Two numbers $a, b \in \mathbb{N}$ are relatively prime (aka coprime) if $(a, b) = 1$

Feb 27-23:29

Example 1

Write $(30, 42)$ in the form $30x + 42y$, stating the values of x and y.

$$42 = 30 . 1 + 12 \qquad (42, 30) = (30, 12)$$

$$30 = 12 . 2 + 6 \qquad (30, 12) = (12, 6)$$

$$12 = 6 . 2 + 0 \qquad (12, 6) = (6, 0) = 6$$

$$\therefore \quad \underline{(42, 30) = 6}$$

Solving for the remainders above gives,

$$12 = 42 - 30 . 1$$

$$6 = 30 - 12 . 2$$

$$\therefore \quad 6 = 30 - (42 - 30 . 1) . 2$$

$$\Rightarrow \quad 6 = 30 - 42 . 2 + 30 . 2$$

$$\Rightarrow \quad 6 = 30 . 3 - 42 . 2$$

$$\therefore \quad \boxed{(30, 42) = 30x + 42y \ (x = 3, y = -2)}$$

Oct 2-23:10

Example 2

Determine whether or not 4 and 7 are coprime.

$$7 = 4 . 1 + 3 \qquad (7, 4) = (4, 3)$$

$$4 = 3 . 1 + 1 \qquad (4, 3) = (3, 1)$$

$$3 = 1 . 3 + 0 \qquad (3, 1) = 1$$

$$\therefore \quad \underline{(4, 7) = 1}$$

$\boxed{\text{As } (4, 7) = 1, 4 \text{ and } 7 \text{ are coprime}}$

AH Maths - MiA (2^{nd} Edn.)

- pg. 318 Ex. 16.3 Q 1 a-c.
- pg. 320 Ex. 16.4 Q 1-4.

Ex. 16.3

1 Find the GCD of each of these pairs of numbers using the Euclidean algorithm.

a 111 and 481 b 451 and 168 c 679 and 388

Ex. 16.4

1 Find the greatest common divisor of 345 and 285 and express it in the form $345s + 285t$, where $s, t \in \mathbb{Z}$.

2 Calculate (583, 318) and express it in the form $583s + 318t$, where $s, t \in \mathbb{Z}$.

3 a Evaluate $d = (1292, 1558)$.

b Hence, express d in the form $1292s + 1558t$ where $s, t \in \mathbb{Z}$.

4 a Show that 763 and 662 are relatively prime.

b Use this fact to express 1 as the sum of multiples of 763 and 662.

c Repeat this for the numbers 1479 and 1178.

Answers to AH Maths (MiA), pg. 318, Ex. 16.3

1 a 37 b 1 c 97

Answers to AH Maths (MiA), pg. 320, Ex. 16.4

1 15; $5 \,.\, 345 - 6 \,.\, 285 = 15$

2 53; $2 \,.\, 318 - 1 \,.\, 583 = 53$

3 a 38 b $5 \,.\, 1558 - 6 \,.\, 1292$

4 a GCD = 1 b $59 \,.\, 763 - 68 \,.\, 662$

c $398 \,.\, 1178 - 317 \,.\, 1479$