Further Number Theory

The Division Algorithm

The division algorithm uses a theorem & method so as to express any given integer *a* as $a = bq + r$, $0 \le r < b$, where $b \ne 0$, $a, b \in \mathbb{Z}^+$ $q \,\&\, r$ are unique.

Examples

Find $q \,\&\, r$ by the division algorithm such that $a = bq + r$ where

① $a = 33 \,\&\, b = 4$

$33 = 4q + r$
$33 = 4 \times 8 + 1$
$\therefore q = 8, r = 1$

② $a = 140 \,\&\, b = 6$

$140 = 6q + r$
$140 = 6 \times 23 + 2$
$\therefore q = 23, r = 2$

Questions

Use the division algorithm to find $q \,\&\, r$ such that $a = bq + r$ where

1) $a = 25 \,\&\, b = 7$ 2) $a = 9 \,\&\, b = 4$ 3) $a = 203 \,\&\, b = 8$ 4) $a = 150 \,\&\, b = 6$

Solutions

1)
$a = bq + r$
$25 = 7q + r$
$25 = 7 \times 3 + 4$

$q = 3, r = 4$

2)
$a = bq + r$
$9 = 4q + r$
$9 = 4 \times 2 + 1$

$q = 2, r = 1$

3)
$a = bq + r$
$203 = 8q + r$
$203 = 8 \times 25 + 3$

$q = 25, r = 3$

4)
$a = bq + r$
$150 = 6q + r$
$150 = 6 \times 25 + 0$

$q = 25, r = 0$

Proof of the Division Algorithm

Either *a* is a multiple of *b* $\therefore \exists q \in \mathbb{Z}$ *s.t.* $a = bq$ & $r = 0$.

<u>OR</u> *a* lies between two consecutive multiples of *b* $\therefore bq < a$ and $\therefore a < b(q+1), q \in \mathbb{Z}$.

$bq < a < b(q+1)$

$\Rightarrow 0 < a - bq < bq + b - bq$ $\qquad a - bq = r$
$\Rightarrow 0 < a - bq < b$
$\Rightarrow 0 < r < b$ $\qquad \therefore 0 \le r < b$

The Euclidean Algorithm

The Euclidean Algorithm involves using repeated applications of the division algorithm to find the greatest common divisor of two integers. It is best shown by example.

Examples

① Find the greatest common divisor of 146 & 14.

$146 = 14.10 + 6 \quad \Rightarrow \quad (146,14) = (14,6)$ {This is alternative notation}

$14 = 6.2 + 2 \qquad (14,6) = (6,2)$

$6 = 2.3 + 0 \qquad (6,2) = (2,0)$

$\therefore (146,14) = 2$

② Find (353, 54) & comment on your result.

$353 = 54.6 + 29$

$54 = 29.1 + 25 \qquad (353,14) = 1$

$29 = 25.1 + 4 \qquad \therefore$ Numbers are said to be coprime.

$25 = 4.6 + 1$

$4 = 1.4 + 0$

Questions

1. Find the gcd of

   a) 181 & 481 b) 1246 & 242 c) 2488 & 1040 d) 679 & 388

2. Find the gcd of 264, 186 & 368 by a) Finding the gcd of 186 & 264
   b) Finding the gcd of solution to a) & 368.

Solutions

1.

a)
$481 = 181.2 + 119$
$181 = 119.1 + 62$
$119 = 62.1 + 57$
$62 = 57.1 + 5$
$57 = 5.11 + 2$
$5 = 2.2 + 1$
$2 = 1.2 + 0$
$\therefore \text{gcd} = 1$

b)
$1246 = 242.5 + 36$
$242 = 36.6 + 26$
$36 = 26.1 + 10$
$26 = 10.2 + 6$
$10 = 6.1 + 4$
$6 = 4.1 + 2$
$4 = 2.2 + 0$
$\therefore \text{gcd} = 2$

c)
$2488 = 1040.2 + 408$
$1040 = 408.2 + 224$
$408 = 224.1 + 184$
$224 = 184.1 + 40$
$184 = 40.4 + 24$
$40 = 24.1 + 16$
$24 = 16.1 + 8$
$16 = 8.2 + 0$
$\therefore \text{gcd} = 8$

d)
$679 = 388.1 + 291$
$388 = 291.1 + 97$
$291 = 97.3$
$\therefore \text{gcd} = 97$

2. a) $264 = 186.1 + 78$
$186 = 78.2 + 30$
$78 = 30.2 + 18$
$30 = 18.1 + 12$
$18 = 12.1 + 6$
$12 = 6.2 + 0$
$\therefore \text{gcd} = 6$

b) $368 = 6.61 + 2$
$6 = 2.3 + 0$
$\therefore \text{gcd} = 2$

<u>Using the Euclidean Algorithm</u>

The Euclidean Algorithm can be used to express a gcd as a linear combination of two integers.

<u>Examples</u>

① Find $a, b \in \mathbb{Z}$ such that $280a + 117b = 1$.

Perform the Euclidean Algorithm	Rearrangement
$280 = 117.2 + 46$	$46 = 280 - 2.117$
$117 = 46.2 + 25$	$25 = 117 - 2.46$
$46 = 25.1 + 21$	$21 = 46 - 1.25$
$25 = 21.1 + 4$	$4 = 25 - 1.21$
$21 = 4.5 + 1$	$1 = 21 - 5.4$
$4 = 1.4 + 0$	
$\therefore \text{gcd} = 1$	

Work backwards to achieve linear combination

$1 = 21 - 5.4$
$1 = 21 - 5.(25 - 1.21)$
$1 = 21 + 5.21 - 5.25$
$1 = 6.21 - 5.25$
$1 = 6.(46 - 1.25) - 5.25$
$1 = -11.25 + 6.46$
$1 = -11.(117 - 2.46) + 6.46$
$1 = -11.117 + 28.46$
$1 = -11.117 + 28.(280 - 2.117)$
$1 = 28.28 - 67.117$

$\therefore 280a + 117b = 1$ when $a = 28, b = -67$. (You can check this numerically)

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

$583 = 318.1 + 265$
$318 = 265.1 + 53$
$265 = 53.5 + 0$

$265 = 583 - 1.318$
$53 = 318 - 1.265$

$53 = 318 - 1.(583 - 1.318)$
$53 = 2.318 - 1.583$

$\therefore \text{gcd} = 53$ $\quad \therefore s = -1, t = 2$ $\quad 583s + 318t = 53$

③ $5612x + 540y = 4$. Assuming $x, y \in \mathbb{Z}$, find their values.

$5612 = 540.10 + 212$
$540 = 212.2 + 116$
$212 = 116.1 + 96$
$116 = 96.1 + 20$
$96 = 20.4 + 16$
$20 = 16.1 + 4$
$16 = 4.4 + 0$

$212 = 5612 - 10.540$
$116 = 540 - 2.212$
$96 = 212 - 1.116$
$20 = 116 - 1.96$
$16 = 96 - 4.20$
$4 = 20 - 1.16$

$4 = 20 - 1.16$
$4 = 20 - (96 - 4.20)$
$4 = 5.20 - 1.96$
$4 = 5(116 - 1.96) - 1.96$
$4 = 5.116 - 6.96$
$4 = 5.116 - 6(212 - 1.116)$
$4 = 11.116 - 6.212$
$4 = 11(540 - 2.212) - 6.212$
$4 = 11.540 - 28.212$
$4 = 11.540 - 28(5612 - 10.540)$
$4 = 291.540 - 28.5612$

$\therefore x = -28, y = 291.$

④ a) Evaluate $d = (1292, 1558)$.
b) Hence express d in the form $1292x + 1558y$ where $x, y \in \mathbb{Z}$.

a) $1558 = 1292.1 + 266$
$1292 = 266.4 + 228$
$266 = 228.1 + 38$
$228 = 38.6 + 0$

$266 = 1558 - 1.1292$
$228 = 1292 - 4.266$
$38 = 266 - 1.228$

$\therefore \text{gcd} = 38$

b) $38 = 266 - (1292 - 4.266)$
$38 = 5.(1558 - 1.1292) - 1.1292$
$38 = 5.1558 - 6.1292$

$\Rightarrow 1292x + 1558y = 38$ when $x = -6$ and $y = 5$.

Number Bases

Our standard base is base ten.

46 741

$10^4 \quad 10^3 \quad 10^2 \quad 10^1 \quad 10^0$

$$4\times10000+6\times1000+7\times100+4\times10+1\times1$$

This is the decimal system.
We can use the division algorithm to convert a number into another base. The most common are:

Binary – base two, using only the integers 0 & 1.

Octal – base eight, using the integers 0-7.

Hexadecimal – base sixteen, using the integers 0-9 & A, B, C, D, E, F.

There are others; base three is **tenary**, base twelve is **duodecimal**.

Binary

101101 is 45. Why?

$$\begin{aligned}&1.2^5+0.2^4+1.2^3+1.2^2+0.2^1+1.2^0\\&=32+8+4+1\\&=45\end{aligned}$$

We can use the division algorithm to convert 45 into binary.
Bear in mind binary is base **2**.

①
$$\begin{aligned}45&=22.2+1\\22&=11.2+0\\11&=5.2+1\\5&=2.2+1\\2&=1.2+0\\1&=0.2+1\end{aligned}$$

↑ Read upwards for binary number

101101

Convert 57 into binary.

②
$$\begin{aligned}57&=28.2+1\\28&=14.2+0\\14&=7.2+0\\7&=3.2+1\\3&=1.2+1\\1&=0.2+1\end{aligned}$$

111001

Questions

Convert the following numbers into binary numbers

a) 131 b) 17 c) 49 d) 100 e) 432.

Octal

The octal number system work in a similar way. Bear in mind it has a base of 8 and so we will use the numbers 0 to 7.

Examples

① $135 = 16.8 + 7$
$16 = 2.8 + 0$
$2 = 0.8 + 2$

207

② $613 = 76.8 + 5$
$76 = 9.8 + 4$
$9 = 1.8 + 1$
$1 = 0.8 + 1$

1145

Questions

Find the octal form of the following numbers.

a) 439 b) 642 c) 17 d) 200 e) 1964 f) 3024

Hexadecimal

Hexadecimal is again similar, using base 16. From remainder 10 onwards we use letters:

A=10 B=11 C=12 D=13 E=14 F=15.

Examples

Find the hexadecimal form of

① $2167 = 135.16 + 7$
$135 = 8.16 + 7$
$8 = 0.16 + 8$

877

② $974 = 60.16 + 14 \Rightarrow E$
$60 = 3.16 + 12 \Rightarrow C$
$12 = 0.16 + 3$

3CE

Questions

Find the hexadecimal numbers equivalent to;

a) 6015 b) 579 c) 3114 d) 8163 e) 1001 f) 369

Past Paper Questions

2001 – B1

Use the Euclidean algorithm to find integers x and y such that $149x+139y=1$.

(4 marks)

2004 – Q8

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 $231x+17y=1$. **(4 marks)**

2007 – Q7

Use the Euclidean algorithm to find integers p & q such that $599p+53q=1$.

(4 marks)

2012 – Q10

Use the division algorithm to express 1234_{10} in base 7. **(3 marks)**

2013 – Q5

Use the Euclidean algorithm to obtain the greatest common divisor of 1204 and 833, expressing it in the form $1204a+833b$, where a and b are integers.

(4 marks)

2015 – Q7

Use the Euclidean algorithm to find integers p and q such that

$$3066p+713q=1.$$ **(4 marks)**

2017 – Q8

Use the Euclidean algorithm to find integers a and b such that

$$1595a+1218b=29.$$ **(4 marks)**