28 / 2 / 18

Number Theory - Lesson 2

The Fundamental Theorem of Arithmetic and Number Bases

LI

- Know and use the FTA.
- Write numbers in different bases.

SC

- Euclidean algorithm.

The Fundamental Theorem of Arithmetic (FTA) states that every integer can be written as a product of prime powers in exactly one way

For example,

$$9 = 3^2$$

$$488 = 2^3 \times 61$$

Example 1

Prove that $\sqrt{2}$ is irrational using the FTA.

Assume that $\sqrt{2}$ is rational. Then $\exists\, a, b \in \mathbb{Z}$ $(b \neq 0)$ such that,

$$\sqrt{2} = \frac{a}{b}$$

where it can be assumed that a and b have no common factors; if they did, they can be cancelled out. Then,

$$a^2 = 2b^2$$

By the FTA, a and b can be written uniquely as a product of primes. So,

$$(m_1 m_2 \ldots m_s)^2 = 2(n_1 n_2 \ldots n_t)^2$$

$$\Rightarrow \quad \underline{m_1^2 m_2^2 \ldots m_s^2 = 2 n_1^2 n_2^2 \ldots n_t^2}$$

The LHS of the previous equation has $2s$ factors, but the RHS has $2t + 1$ factors. This cannot happen if the two sides are equal.

$\boxed{\text{By contradiction, } \sqrt{2} \text{ is irrational}}$

Any number A can be written as uniquely as base n as,

$$A = \sum_{r=0}^{n} r_{k-i}\, n^{k-i} = (r_k\, r_{k-i} \ldots r_2\, r_1\, r_0)_n$$

Sometimes the brackets are omitted

by dividing A (and all subsequent quotients) by n and obtaining the remainders until a 0 remainder is left. The number A is often written as,

$$A = r_k n^k + r_{k-1} n^{k-1} + \ldots + r_2 n^2 + r_1 n^1 + r_0 n^0$$

For example, 6 402 can be written in base 10 as,

$$6\,402 = 6 \,.\, 10^3 + 4 \,.\, 10^2 + 0 \,.\, 10^1 + 2 \,.\, 10^0$$
$$= (6402)_{10}$$

For example, 37 can be written in base 2 as,

$$37 = 1 \,.\, 2^5 + 0 \,.\, 2^4 + 0 \,.\, 2^3 + 1 \,.\, 2^2 + 0 \,.\, 2^1 + 1 \,.\, 2^0$$
$$= (100101)_2$$

Example 2

Write $(2031)_5$ in base 10.

$$(2031)_5 = 2 . 5^3 + 0 . 5^2 + 3 . 5^1 + 1 . 5^0$$

$$\Rightarrow \quad (2031)_5 = 2 . 125 + 0 + 15 + 1$$

$$\Rightarrow \quad \boxed{(2031)_5 = (266)_{10}}$$

Oct 2-23:10

Example 3

Change $(8469)_{10}$ to base 7.

$8\,469 \div 7 = 1\,209$ remainder 6 $(= r_0)$.

$1\,209 \div 7 = 172$ remainder 5 $(= r_1)$.

$172 \div 7 = 24$ remainder 4 $(= r_2)$.

$24 \div 7 = 3$ remainder 3 $(= r_3)$.

$3 \div 7 = 0$ remainder 3 $(= r_4)$.

$$\therefore \quad \boxed{(8469)_{10} = (33456)_7}$$

For number bases bigger than 10, we need to invent new symbols for the bigger numbers. For example, in base 13, A is 10, B is 11, C is 12 etc.. Other letters may be used for these.

To convert from one non-base ten number to another non-base ten number, we go through base 10.

Example 4

Change $(8A69)_{12}$ to base 5 $(A = 10)$.

First convert to base 10.

$$(8A69)_{12} = 8 \,.\, 12^3 + 10 \,.\, 12^2 + 6 \,.\, 12^1 + 9 \,.\, 12^0$$

$$\Rightarrow \quad (8A69)_{12} = 13\,824 + 1\,440 + 72 + 9$$

$$\Rightarrow \quad \underline{(8A69)_{12} = (15345)_{10}}$$

Now convert this to base 5.

$15\,345 \div 5 = 3\,069$ remainder 0 $(= r_0)$.

$3\,069 \div 5 = 613$ remainder 4 $(= r_1)$.

$613 \div 5 = 122$ remainder 3 $(= r_2)$.

$122 \div 5 = 24$ remainder 2 $(= r_3)$.

$24 \div 5 = 4$ remainder 4 $(= r_4)$.

$4 \div 5 = 0$ remainder 4 $(= r_5)$.

$$\therefore \quad \boxed{(8A69)_{12} = (442340)_5}$$

Oct 2-23:10

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

- pg. 315 - 6 Ex. 16.2 Q 5, 9, 10.
- pg. 322 - 4 Ex. 16.5 Q 1, 2.

Ex. 16.2

5 Use the unique factorisation theorem to prove

a $\sqrt{7}$ is irrational b $\sqrt{p}$ is irrational where p is a prime.

9 Prove that there are no integers x and y such that $6^x = 21^y$.

10 Prove $\log_{10} 5$ is irrational by

a assuming it is rational

b using the laws of logs to show some power of 10 is equal to a power of 5

c using the unique factorisation theorem

Ex. 16.5

1 Express these numbers in base 10.

a 1234_7 b 777_8 c 110110_2

d $t81e_{12}$ where t and e are digits representing 10 and 11 respectively.

2 Change these numbers to the base indicated.

a 63_{10} to base 2 b 333_{10} to base 4 c 1727_{10} to base 12

d 626_7 to base 5 e 401_6 to base 7 f $tt5_{12}$ to base 6

Answers to AH Maths (MiA), pg. 315-6, Ex. 16.2

5 **a** $\sqrt{7} = \frac{m}{n} \Rightarrow 7n^2 = m^2$: LHS has odd number of prime factors; RHS has even.

b $\sqrt{p} = \frac{m}{n} \Rightarrow pn^2 = m^2$: LHS has odd number of prime factors; RHS has even.

9 $6^x = 2^x 3^x; 21^y = 3^y 7^y$

By unique factorization theorem $6^x \neq 21^y$

10 $\log_{10} 5 = \dfrac{m}{n} \Rightarrow 5 = 10^{\frac{m}{n}} \Rightarrow 5^n = 10^m \Rightarrow 5^n = 2^m \,.\, 5^m$

$\Rightarrow 5^{n-m} = 2^m$

By unique factorization theorem $5^{n-m} \neq 2^m$

Answers to AH Maths (MiA), pg. 322-4, Ex. 16.5

1 **a** 466 **b** 511 **c** 54 **d** 18 455

2 **a** 111111_2 **b** 11031_4

c eee_{12} **d** 2224_5

e 265_7 **f** 11125_6