

Tutorial 1

Part A: Binary and Decimal Conversion

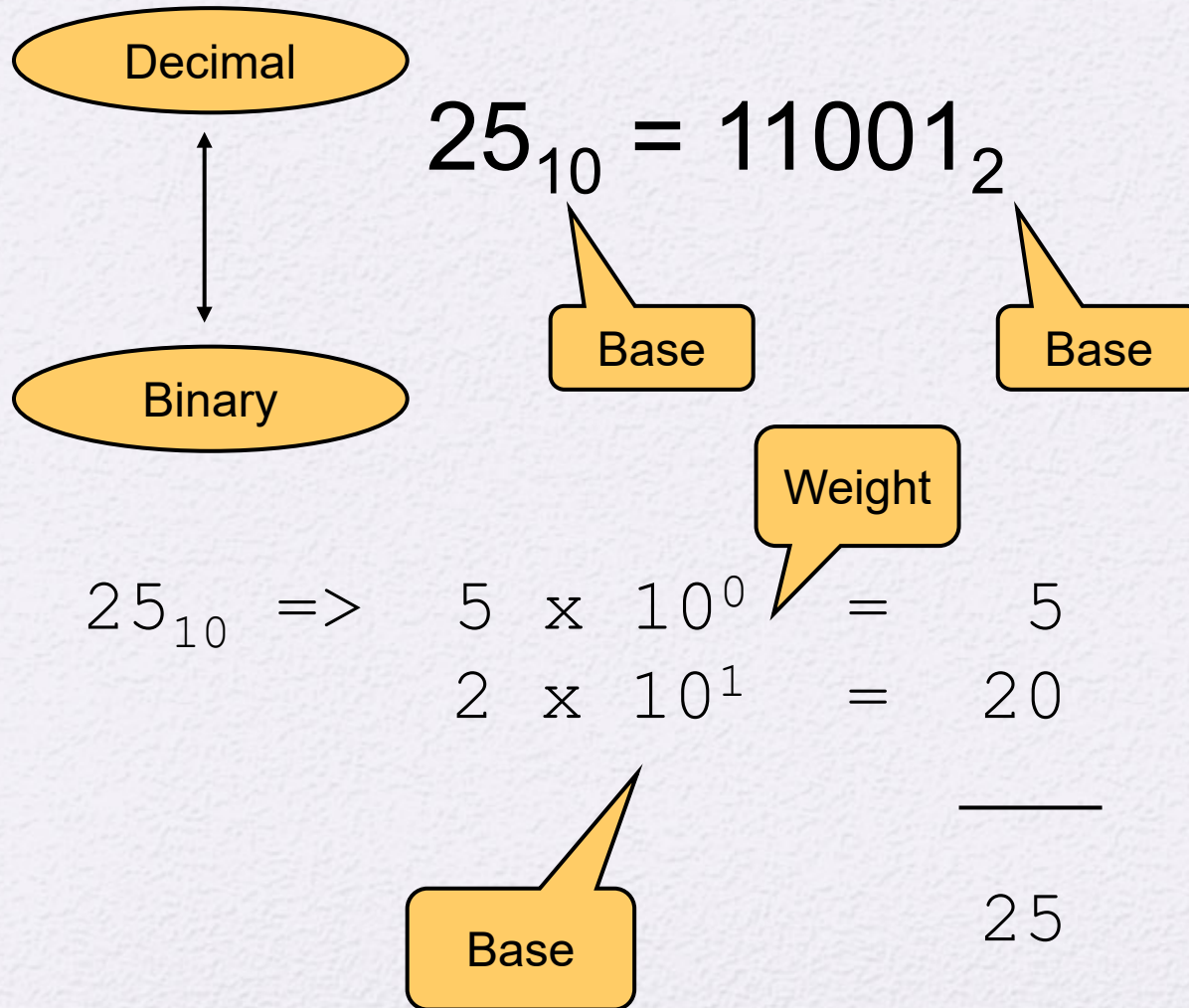
Common Number Systems

System	Base	Symbols	Used by humans?	Used in computers?
Decimal	10	0, 1, ... 9	Yes	No
Binary	2	0, 1	No	Yes

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111

Decimal	Binary
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

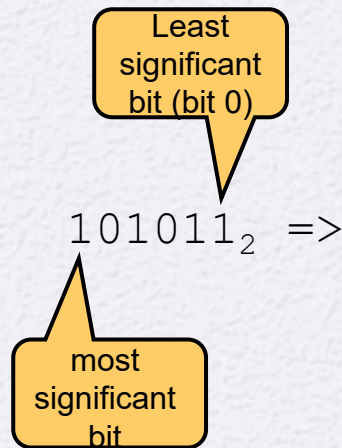
Conversion Among Bases: Example



Binary to Decimal

- How?

- Multiply each bit by 2^n , where n is the “position” of the bit starting from 0 on the right
- Add the results

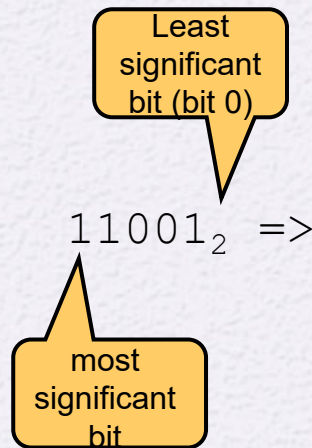


1	x	2 ⁰	=	1
1	x	2 ¹	=	2
0	x	2 ²	=	0
1	x	2 ³	=	8
0	x	2 ⁴	=	0
1	x	2 ⁵	=	32
				<hr/>
				43 ₁₀

Binary to Decimal (Example 2)

- How?

- Multiply each bit by 2^n , where n is the “position” of the bit starting from 0 on the right
- Add the results



1	x	2 ⁰	=	1
0	x	2 ¹	=	0
0	x	2 ²	=	0
1	x	2 ³	=	8
1	x	2 ⁴	=	16
				<hr/>
				25 ₁₀

Decimal to Binary

- Technique
 - Divide the decimal number by two, keep track of the remainder
 - First remainder is bit 0 (LSB, least-significant bit)
 - Second remainder is bit 1 and so on
 - Repeat until the quotient is zero which completes the conversion.
 - The last remainder is most-significant bit: MSB

Decimal to Binary Conversion

Example:

Convert the decimal number 6_{10} into its binary equivalent.

$$\begin{array}{r} 3 \\ 2 \overline{) 6} \end{array} \quad r = 0 \leftarrow \text{Least Significant Bit}$$

$$\begin{array}{r} 1 \\ 2 \overline{) 3} \end{array} \quad r = 1$$

$$\begin{array}{r} 0 \\ 2 \overline{) 1} \end{array} \quad r = 1 \leftarrow \text{Most Significant Bit}$$

$$6_{10} = 110_2$$

Dec \rightarrow Binary : Example

Example:

Convert the decimal number 26_{10} into its binary equivalent.

Solution:

$$2 \overline{) 26} \quad r = 0 \leftarrow \text{LSB}$$

$$2 \overline{) 13} \quad r = 1$$

$$2 \overline{) 6} \quad r = 0$$

$$2 \overline{) 3} \quad r = 1$$

$$2 \overline{) 1} \quad r = 1 \leftarrow \text{MSB}$$

$$26_{10} = 11010_2$$

Part 6: Modular Arithmetic

- The modulus
 - If a is an integer and n is a positive integer, we define $a \bmod n$ to be the **remainder** when a is divided by n ; the integer n is called the **modulus**
 - thus, for any integer a :

$$a = qn + r \quad \mathbf{0 \leq r < n}; \quad q = [a/n]$$

$$a = [a/n] * n + (a \bmod n)$$

$$11 \bmod 7 = 4; \quad 15 \bmod 7 = 1$$

Modular Arithmetic

- Congruent modulo n
 - Two integers a and b are said to be **congruent modulo n** if $(a \bmod n) = (b \bmod n)$
 - This is written as $a = b(\bmod n)$

Example

- $a = 17$, $b = 24$ and $n = 7$

Put values in formula

$$(17 \bmod 7) = 3 \text{ and } (24 \bmod 7) = 3$$

Both 17 and 24 have the same remainder (3) when divided by 7, so
 $17 = 24(\bmod 7)$

Modular Arithmetic

- Modular arithmetic exhibits the following properties:
 1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
 2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
 3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

Modular Arithmetic

- Examples:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

$a=11$, $b=15$, and $n=8$

$$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$$

$$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$$

Modular Arithmetic

- Examples:

2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

$a=11$, $b= 15$, and $n=8$

$$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$$

$$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$$

Modular Arithmetic

- Examples:

3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

$a=11$, $b= 15$, and $n=8$

$$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$$

$$(11 * 15) \bmod 8 = 165 \bmod 8 = 5$$

Thanks!