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

Decimal

Binary

$$25_{10} = 11001_2$$

Base

Base

Weight

$$25_{10} \Rightarrow \begin{array}{rcl} 5 \times 10^0 & = & 5 \\ 2 \times 10^1 & = & 20 \\ \hline & & 25 \end{array}$$

Base

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

Least significant bit (bit 0)

most significant bit

101011_2 =>

$$
\begin{aligned}
1 \times 2^0 &= 1 \\
1 \times 2^1 &= 2 \\
0 \times 2^2 &= 0 \\
1 \times 2^3 &= 8 \\
0 \times 2^4 &= 0 \\
1 \times 2^5 &= 32 \\
\hline
& \quad 43_{10}
\end{aligned}
$$

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

Least significant bit (bit 0)

$11001_2 \Rightarrow$

most significant bit

$$
\begin{array}{rcrcr}
1 & \times & 2^0 & = & 1 \\
0 & \times & 2^1 & = & 0 \\
0 & \times & 2^2 & = & 0 \\
1 & \times & 2^3 & = & 8 \\
1 & \times & 2^4 & = & \underline{16} \\
 & & & & 25_{10}
\end{array}
$$

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.

$$2\overline{\smash{)}\,6}^{\,3} \quad r = 0 \leftarrow \text{Least Significant Bit}$$

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

$$2\overline{\smash{)}\,1}^{\,0} \quad r = 1 \leftarrow \text{Most Significant Bit}$$

$6_{10} = 110_2$

Dec → Binary : Example

Example:

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

Solution:

$$2\,\overline{)\,26}^{\;13} \quad r = 0 \leftarrow \text{LSB}$$

$$2\,\overline{)\,13}^{\;6} \quad r = 1$$

$$2\,\overline{)\,6}^{\;3} \quad r = 0$$

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

$$2\,\overline{)\,1}^{\;0} \quad r = 1 \leftarrow \text{MSB}$$

$26_{10} = 11010_2$

Part 6: Modular Arithmetic

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

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

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

11 mod 7 = 4; 15 mod 7 = 1

Modular Arithmetic

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

Example

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

Put values in formula

(17 mod 7) = 3 and (24 mod 7) = 3

Both 17 and 24 have the same remainder (3) when divided by 7, so 17=24(mod 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 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 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 mod 8) - (15 mod 8)] mod 8 = - 4 mod 8 = 4

(11 - 15) mod 8 = - 4 mod 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 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

Thanks!